Version expérimentale
En cours de validation

RÉSUMÉ THÉORIQUE – FILIÈRE SYSTÈMES ET RÉSEAUX

M204 – DÉCOUVRIR LES ENJEUX DE LA TECHNOLOGIE SDN

45 heures

SOMMAIRE

MODALITÉS PÉDAGOGIQUES

1

LE GUIDE DE SOUTIEN

Il contient le résumé théorique et le manuel des travaux pratiques

2

LA VERSION PDF

Une version PDF est mise en ligne sur l'espace apprenant et formateur de la plateforme WebForce Life

3

DES CONTENUS TÉLÉCHARGEABLES

Les fiches de résumés ou des exercices sont téléchargeables sur WebForce Life

4

DU CONTENU INTERACTIF

Vous disposez de contenus interactifs sous forme d'exercices et de cours à utiliser sur WebForce Life

5

DES RESSOURCES EN LIGNES

Les ressources sont consultables en synchrone et en asynchrone pour s'adapter au rythme de l'apprentissage

PARTIE 1

Comprendre les réseaux informatique en nuage

Dans ce module, vous allez :

- Être en mesure de comprendre le concept du cloud networking
- Être en mesure de maitriser les notions de base de la virtualisation des réseaux

22 heures

CHAPITRE 1

Définir le Cloud Networking

Ce que vous allez apprendre dans ce chapitre :

- Comprendre le concept du cloud networking

6 heures

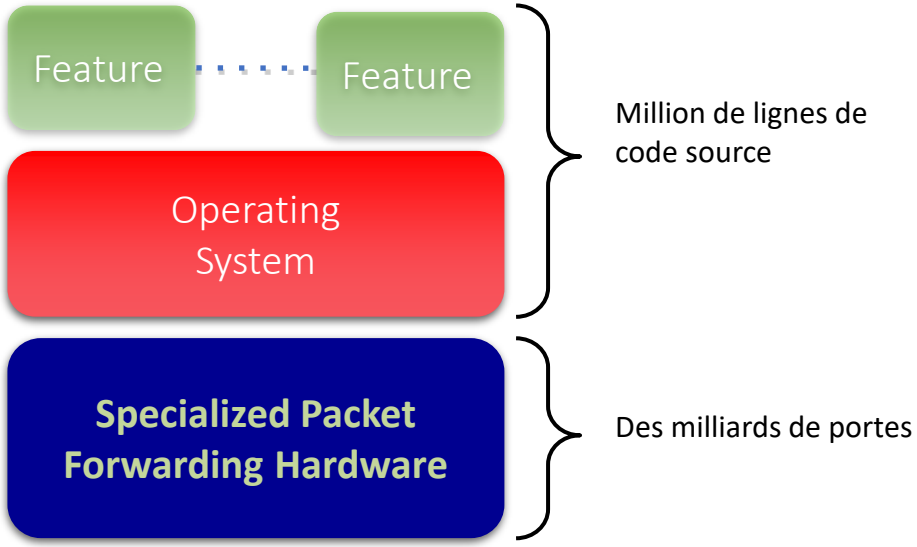
CHAPITRE 1

Comprendre le concept de la virtualisation des réseaux

1. Les limites des réseaux traditionnels
2. Cloud computing et virtualisation
3. Technologies de virtualisation des réseaux

Traditional Network Node (Router Example)

De nombreuses fonctions complexes intégrées à l'infrastructure : *OSPF, BGP, multicast, differentiated services, Traffic Engineering, NAT, firewalls, …*



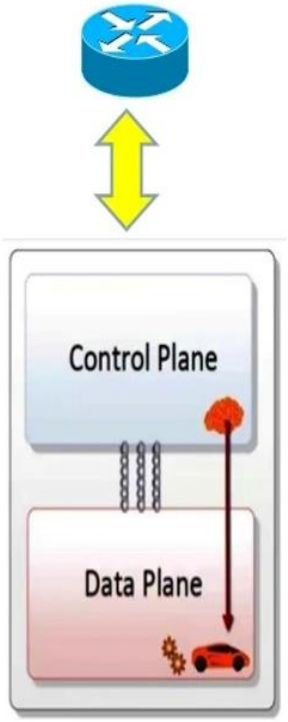
Ne peut pas changer dynamiquement en fonction des conditions du réseau

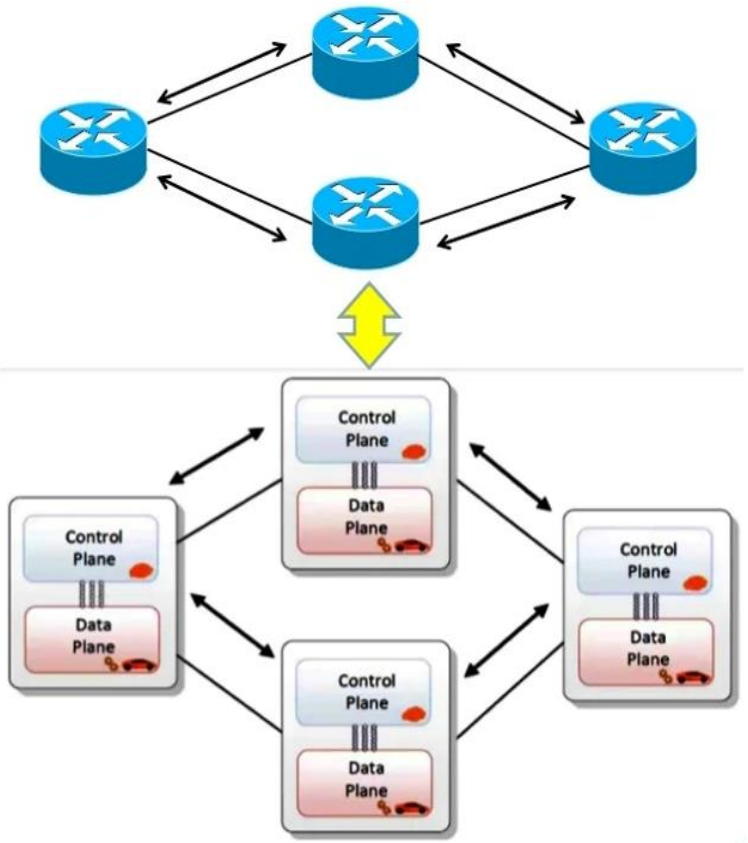
Problématiques des réseaux traditionnels

- Complexité des réseaux traditionnels : l'ajout ou la modification d'équipements et l'implémentation de politiques réseaux sont complexes, longues et peuvent être source d'interruptions de service. Ce qui décourage les modifications et les évolutions du réseau.
- Passage à l'échelle : l'impossibilité d'avoir un réseau qui s'adapte au trafic à obliger les opérateurs de à surprovisionner leurs réseaux.
- Dépendance aux constructeurs : les constructeurs réalisent des produits avec des durées de vie et un manque de standard, d'interface ouverte. Ce qui limite les opérateurs réseaux d'adapter le réseau à leurs propres besoins.

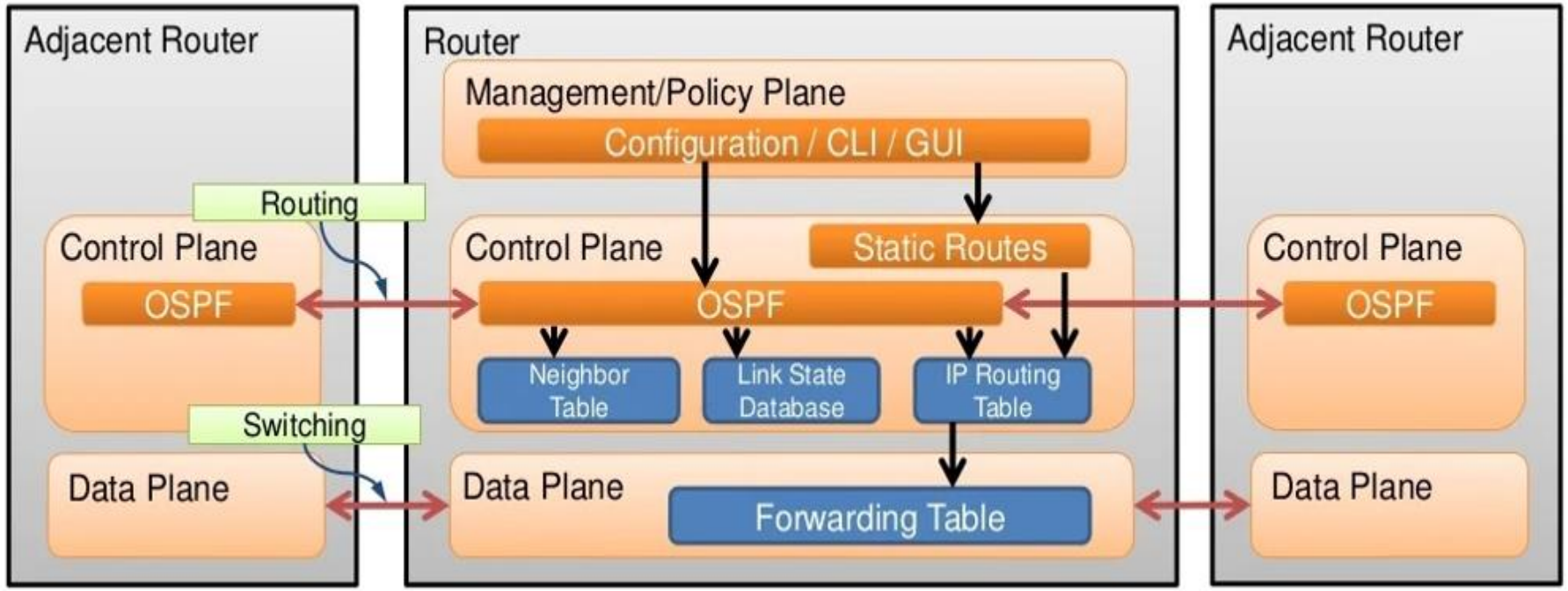
Le réseau traditionnel

- Difficile de réaliser des expériences en conditions réelles sur des réseaux de production à grande échelle. Stagnation de la recherche - équipements coûteux à acquérir et réseaux à mettre en place par chaque équipe pour la recherche Les réseaux sont restés les mêmes pendant de nombreuses années Le taux d'innovation dans les réseaux est plus lent car les protocoles sont définis de manière isolée, faute d'abstraction de haut niveau. Systèmes fermés Difficile de collaborer de manière significative en raison du manque d'interfaces ouvertes standard. Les vendeurs commencent à s'ouvrir mais pas de manière significative. L'innovation est limitée aux fournisseurs/partenaires fournisseurs D'énormes obstacles aux nouvelles idées de réseautage.





Configuration



PARTIE 1

CHAPITRE 1

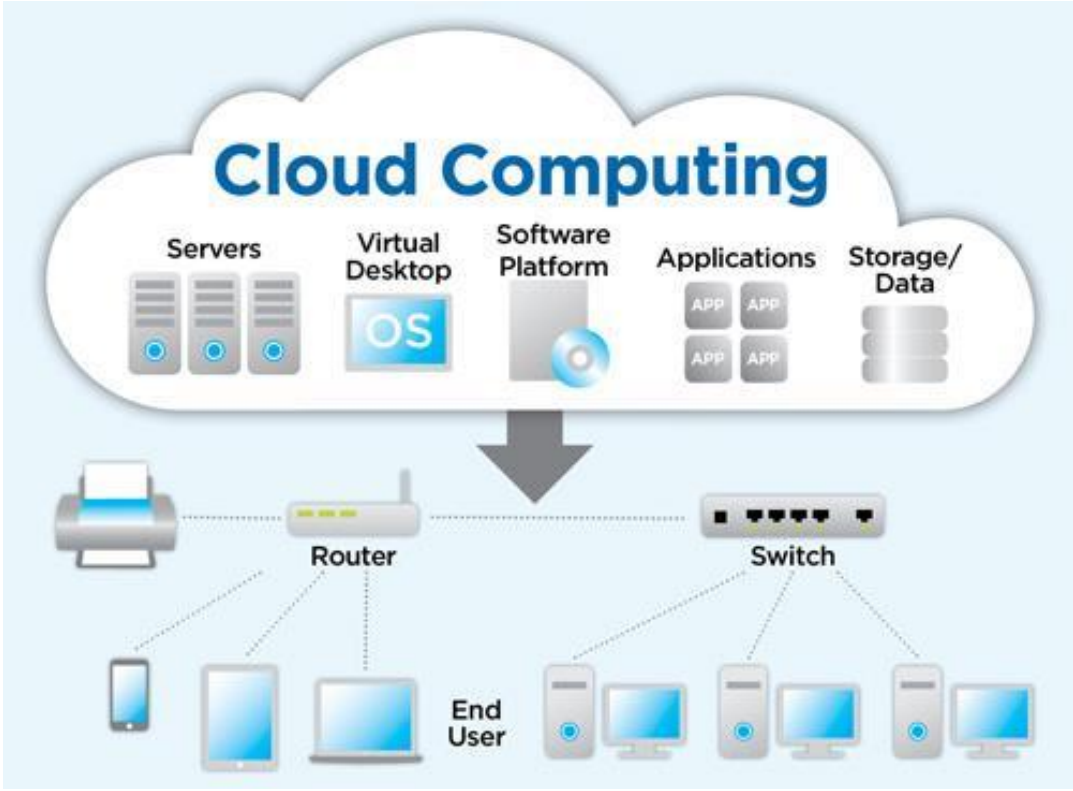
Comprendre le concept de la virtualisation des réseaux

1. Les limites des réseaux traditionnels
2. Cloud computing et virtualisation
3. Technologies de virtualisation des réseaux

Présentation du cloud

Le cloud computing aborde toute une série de questions relatives à la gestion des données :

- Il permet l'accès aux données organisationnelles en tout lieu et à tout moment
- Il rationalise l'organisation des opérations des services informatiques de l'entreprise en leur permettant de s'abonner uniquement aux services requis
- Il réduit, voire supprime, le besoin de disposer des équipements sur site, ainsi que la gestion et la maintenance de ceux-ci
- Il réduit le coût de possession du matériel, les dépenses énergétiques, les besoins d'espace physique ainsi que ceux concernant la formation du personnel
- Il permet aussi une réponse rapide face au besoin croissant d'espace de stockage des données



PARTIE 1

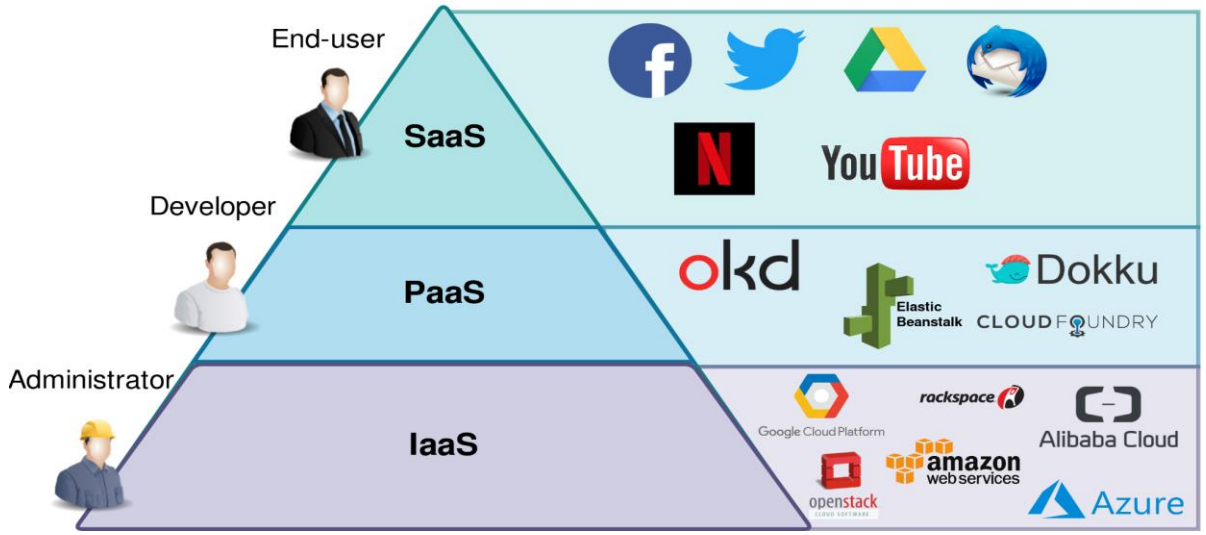
PARTIE 1

Services cloud

Dans son rapport spécial 800-145, le NIST (l'institut américain des normes et de la technologie) a identifié les trois principaux services de cloud computing:

- **SaaS (ou Logiciel en tant que service)** - le fournisseur cloud gère l'accès aux services, tels que la messagerie, les outils de communication et Office 365, qui sont fournis via Internet.
- **PaaS (ou Plate-forme en tant que service)** - le fournisseur cloud gère l'accès aux outils et services de développement utilisés pour fournir les applications aux utilisateurs.
- **IaaS (Infrastructure as a Service)** - Le fournisseur de cloud computing est chargé de donner aux responsables informatiques l'accès à l'équipement réseau, aux services réseau virtualisés et à l'infrastructure réseau de support.

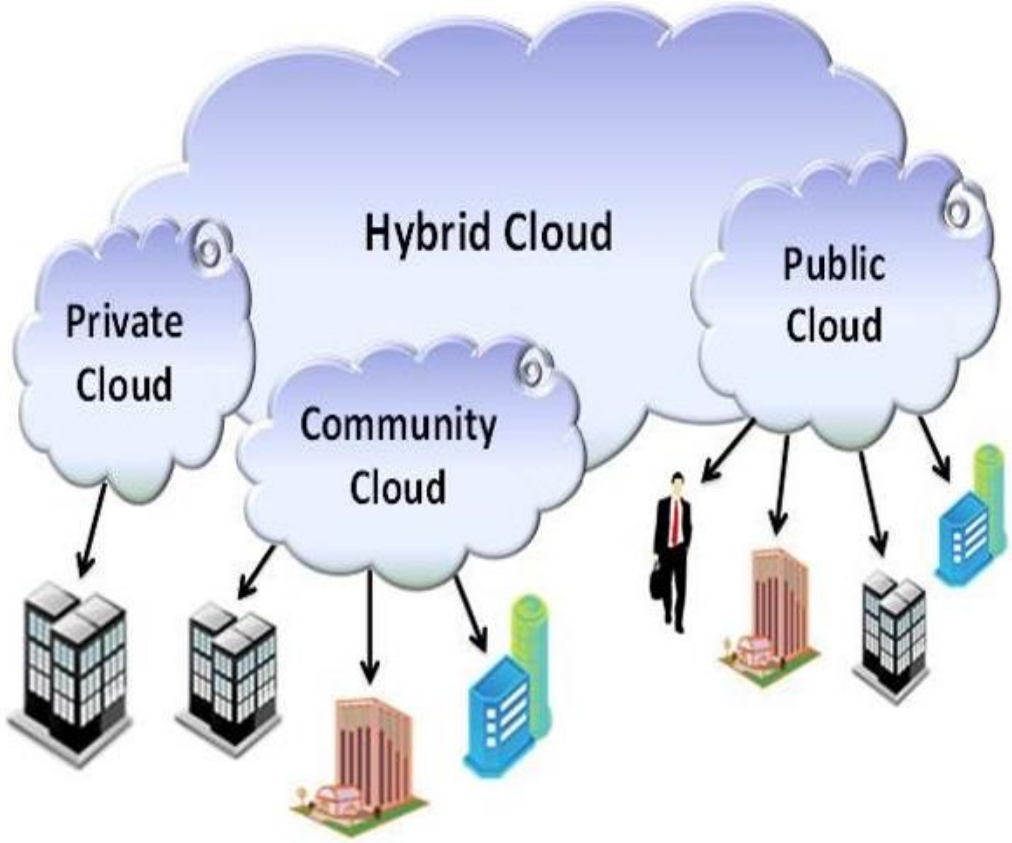
Les fournisseurs de services cloud ont développé ce modèle en y intégrant un support informatique pour chaque service de cloud computing (ITaaS). Pour les entreprises, ITaaS peut étendre la capacité du réseau sans nécessiter d'investissement dans de nouvelles infrastructures, de formation de nouveau personnel ou de licence pour de nouveaux logiciels.



Modèles de cloud

Les quatre principaux modèles cloud sont les suivants:

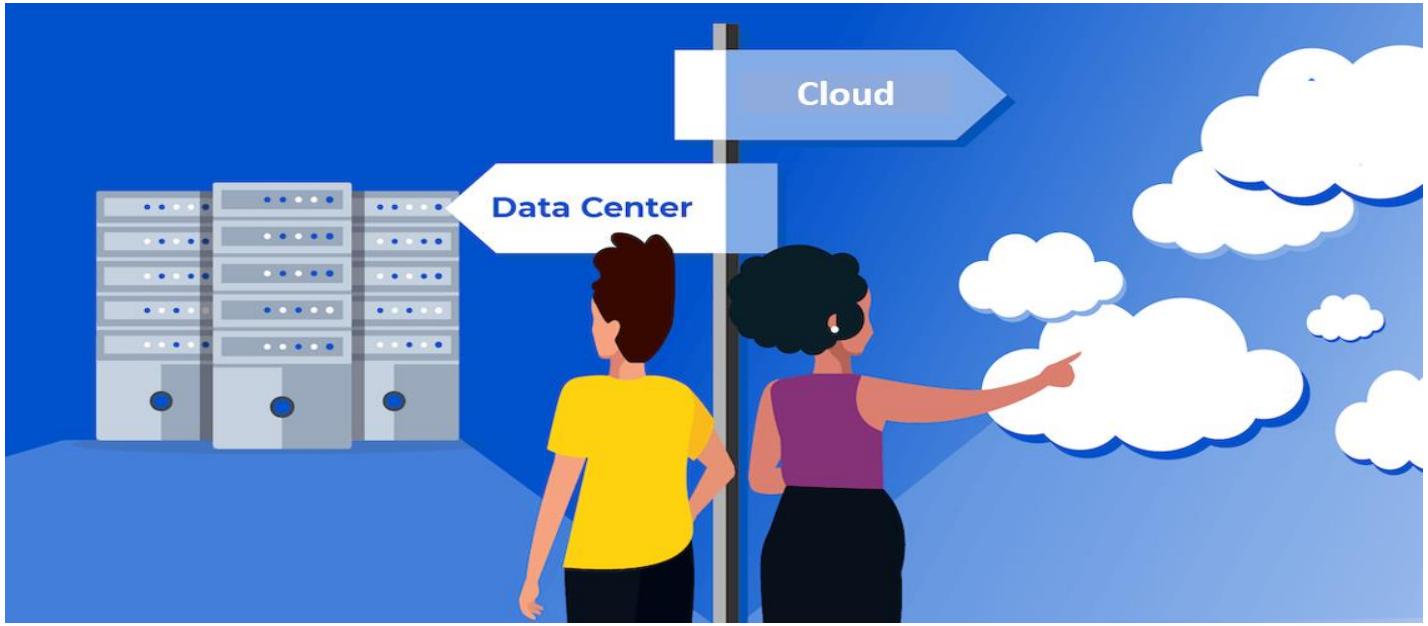
- **Clouds publics** - Des applications et des services basés sur le cloud accessibles par le grand public.
- **Clouds privés** - Des applications et des services basés sur le cloud sont destinés à une entreprise ou à une entité spécifique, par exemple une administration.
- **Clouds hybrides** - Un cloud hybride est constitué de deux ou plusieurs nuages (exemple : partie privée, partie publique), où chaque partie reste un objet distinct, mais où les deux sont reliés par une architecture unique.
- **Clouds communautaires** - L'infrastructure cloud est déployée à l'usage exclusif d'une communauté, d'un ensemble d'entreprises ou d'organisation ayant des intérêts communs. Cette infrastructure peut être gérée par un tiers, une ou plusieurs entreprises/organisations de la communauté.
-



Cloud computing vs Data center

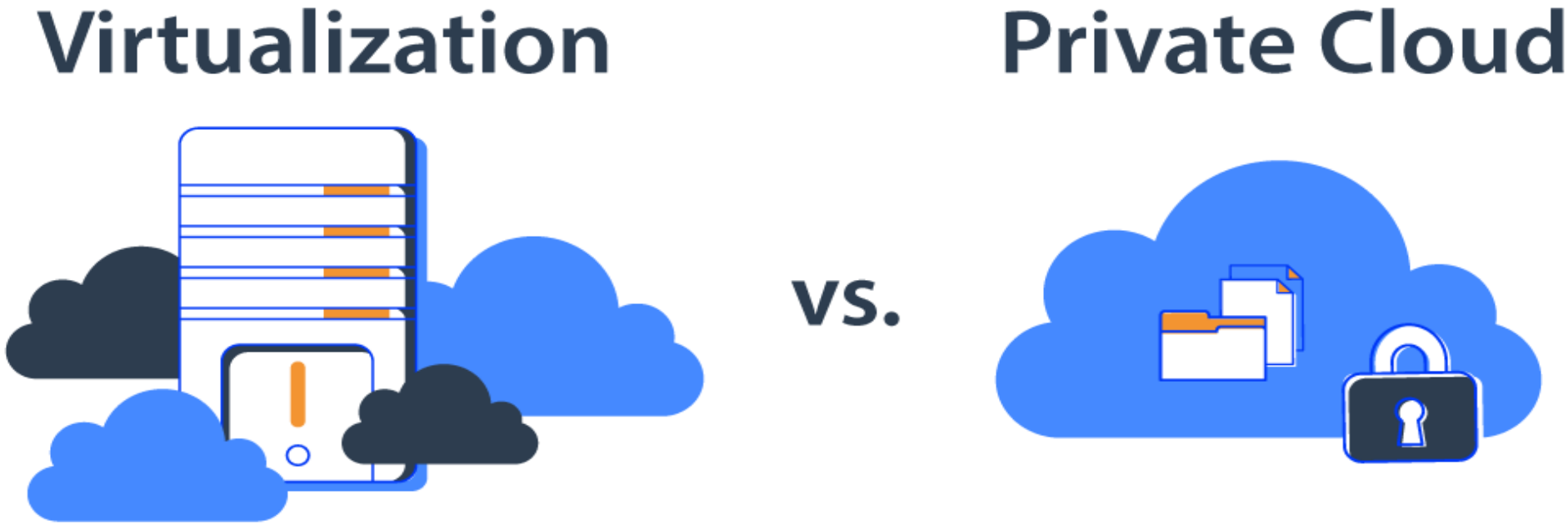
- **Data center**: espace de stockage ou de traitement de données géré par un département informatique interne ou loué hors site. La construction et l'entretien des data centers sont en général très coûteux.
- **Cloud computing**: service hors site qui offre un accès à la demande à un pool partagé de ressources informatiques configurables. Ces ressources peuvent être rapidement mises en service et distribuées avec un minimum d'efforts de gestion.

Les centres de données sont les installations physiques qui répondent aux besoins de calcul, de réseau et de stockage des services de cloud computing. Les fournisseurs de services cloud utilisent les data centers pour héberger leurs services et leurs ressources basés dans le cloud.



Cloud computing vs virtualisation

- Bien qu'on les confonde souvent, les termes « cloud computing » et « virtualisation » font référence à des concepts bien différents. La virtualisation forme le socle du cloud computing. Sans elle, le cloud computing, tel qu'on le connaît, n'existerait pas.
- La virtualisation sépare le système d'exploitation (OS) du matériel. Plusieurs fournisseurs proposent des services cloud virtuels capables de provisionner les serveurs de manière dynamique en fonction des besoins. Ces instances virtualisées de serveurs sont créées à la demande.

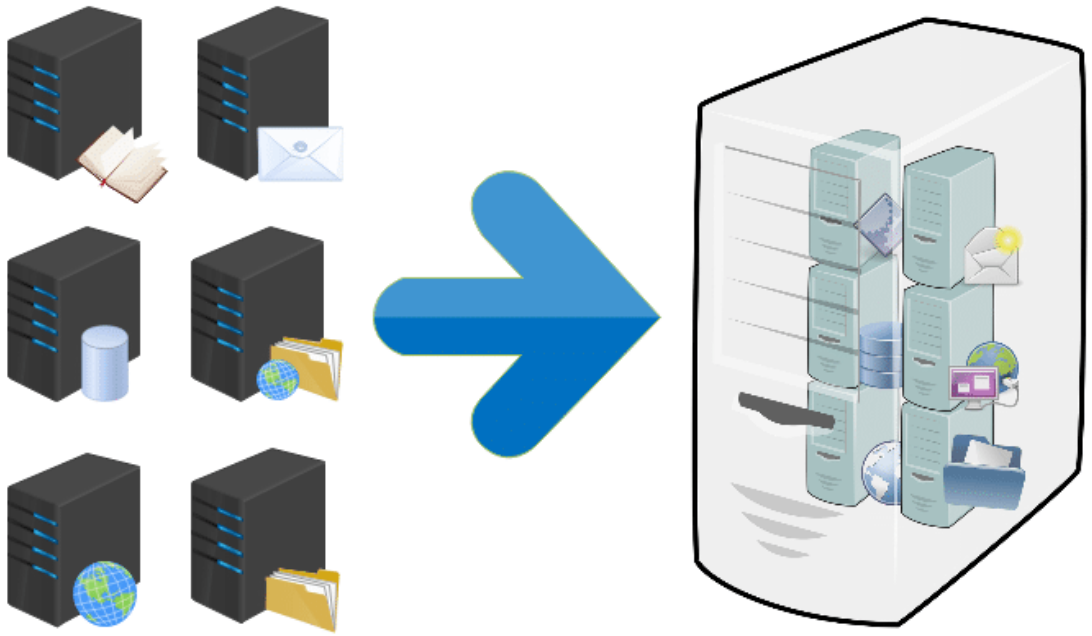


Serveurs dédiés

- Lorsqu'un composant tombe en panne, le service fourni par ce serveur devient indisponible. C'est ce qu'on appelle un « point de défaillance unique ».
- Les serveurs dédiés étaient généralement sous-utilisés. Ils restaient souvent inactifs pendant de longues périodes jusqu'à ce que le service spécifique fourni soit sollicité. Ces serveurs ont gaspillé de l'énergie et pris plus d'espace que ne le justifiait la quantité de services fournis. C'est ce qu'on appelle la prolifération des serveurs.

Virtualization des serveurs

- La virtualisation des serveurs tire parti des ressources inactives pour consolider le nombre de serveurs nécessaires. Ainsi, plusieurs systèmes d'exploitation peuvent coexister sur une plate-forme matérielle unique.
- Pour résoudre le problème de point de défaillance unique, la virtualisation implique généralement une fonction de redondance
- L'hyperviseur est un programme, un firmware ou un équipement matériel qui ajoute une couche d'abstraction au-dessus du matériel physique. La couche d'abstraction permet de créer des machines virtuelles qui ont accès à tous les composants matériels de la machine physique, notamment les processeurs, la mémoire, les contrôleurs de disque et les cartes réseau.



Avantages de la virtualisation

L'un des principaux avantages de la virtualisation est qu'elle permet de réduire le coût global :

- Moins de matériel requis
- Moins d'énergie consommée
- Moins d'espace occupé

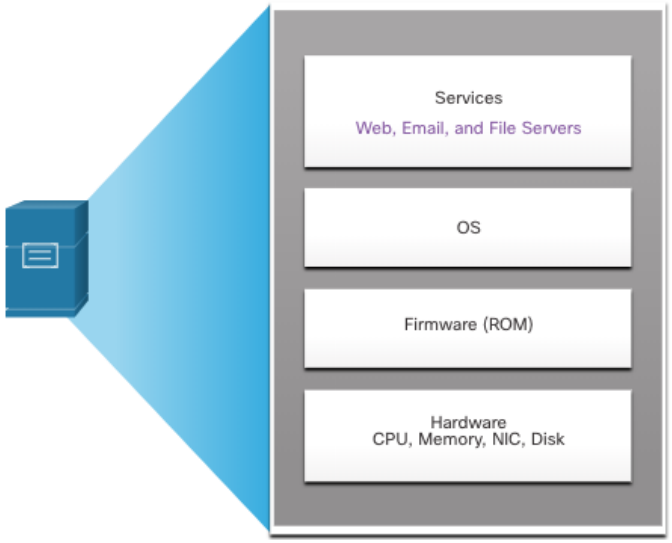
La virtualisation présente également d'autres avantages :

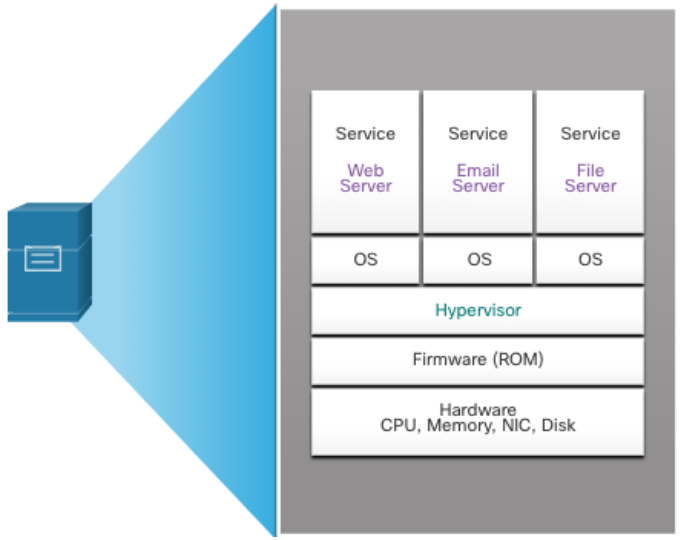
- Prototypage plus facile
- Provisionnement plus rapide des serveurs
- augmentation de la durée de fonctionnement des serveurs
- Meilleure reprise après sinistre
- Prise en charge de l'existant

Couches d'abstraction

Un système informatique se compose des couches d'abstraction suivantes : services, système d'exploitation, micrologiciels et matériel.

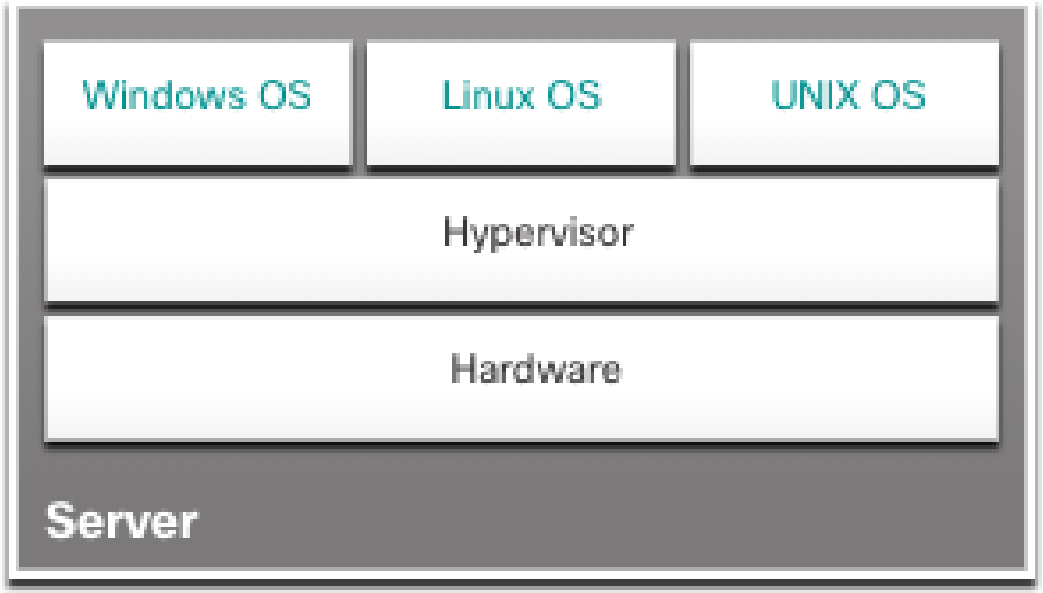
- À chaque couche d'abstraction, un code de programmation sert d'interface entre les couches inférieures et supérieures.
- Un hyperviseur est installé entre le firmware et le système d'exploitation. L'hyperviseur peut prendre en charge plusieurs instances de système d'exploitation.



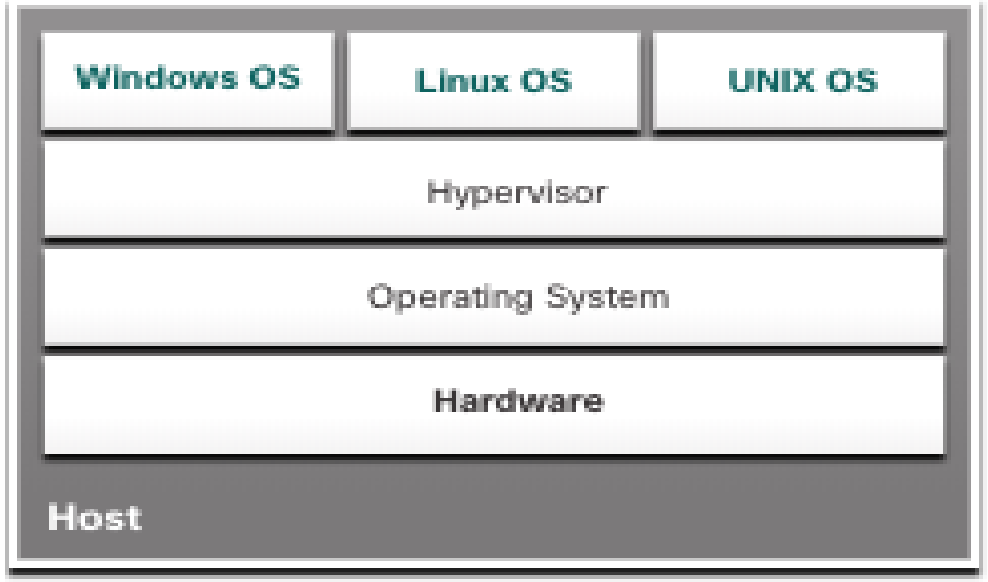


Concept de virtualisation

- **Hyperviseurs de type 1**



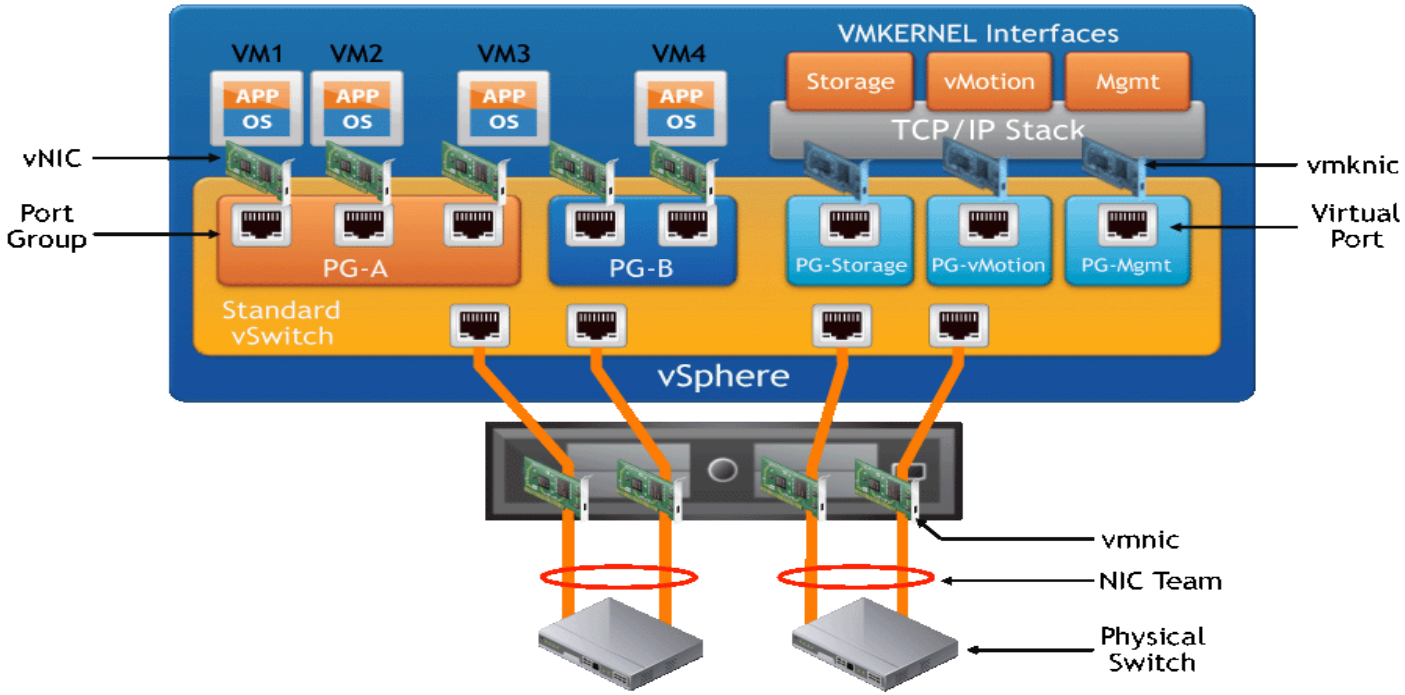
- **Hyperviseurs de type 2**



PARTIE 1

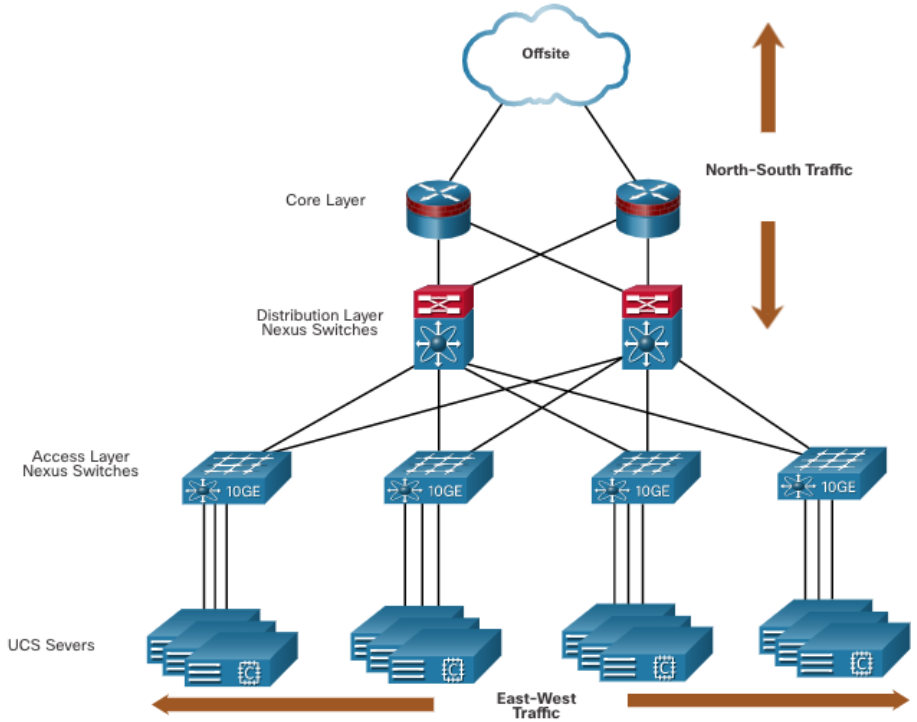
Virtualisation du réseau

- Virtualisation de réseau : Notion d'instanciation de plusieurs réseaux logiques distincts au-dessus d'une seule infrastructure de réseau physique partagée.
- L'infrastructure de réseau peut également tirer parti de la virtualisation. Les fonctions de réseau peuvent être virtualisées.
- Chaque périphérique réseau peut être segmenté en plusieurs périphériques virtuels fonctionnant en tant que périphériques indépendants. Les exemples incluent les sous-interfaces, les interfaces virtuelles, les VLAN et les tables de routage. Le routage virtualisé est appelé routage et transfert virtuels (VRF).
-



La complexité de la virtualisation avec le réseau traditionnel

- Lorsqu'un serveur est virtualisé, ses ressources ne sont pas visibles. Cela peut créer des problèmes lors de l'utilisation d'architectures de réseau traditionnelles.
- Les machines virtuelles peuvent être déplacées, et l'administrateur réseau doit être en mesure d'ajouter, supprimer et modifier des ressources et des profils réseau pour faciliter leur mobilité. Ce processus serait manuel et prendrait beaucoup de temps avec les commutateurs de réseau traditionnels.
- Les flux de trafic diffèrent sensiblement du modèle client-serveur traditionnel. Généralement, il y a un volume considérable de trafic échangé entre des serveurs virtuels (trafic Est-Ouest) qui change de localisation et d'intensité au fil du temps. Le trafic nord-sud est généralement destiné à des emplacements hors site tels qu'un autre centre de données, d'autres fournisseurs de services de cloud ou l'internet.
- Le trafic dynamique en constante évolution nécessite une approche flexible de la gestion des ressources réseau. Pour faire face à ces fluctuations, les infrastructures réseau existantes peuvent s'appuyer sur des configurations de QoS et de niveau de sécurité propres à chaque flux. Néanmoins, dans les grandes entreprises qui utilisent des équipements multifournisseurs, la reconfiguration nécessaire après l'activation d'une nouvelle machine virtuelle risque de prendre beaucoup de temps.



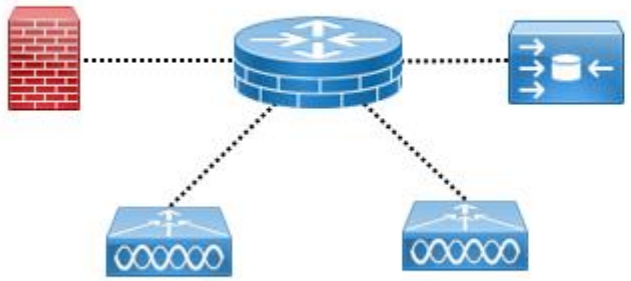
PARTIE 1

Autres challenges sur les sites distants

- la virtualisation sur les sites distants se développe avec de nouveaux challenges :

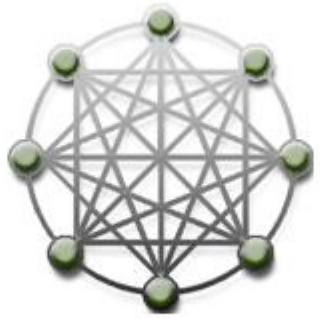
Plusieurs équipements

Routeurs, Appliances, Serveurs



Complexes à manager

Intégration des équipements



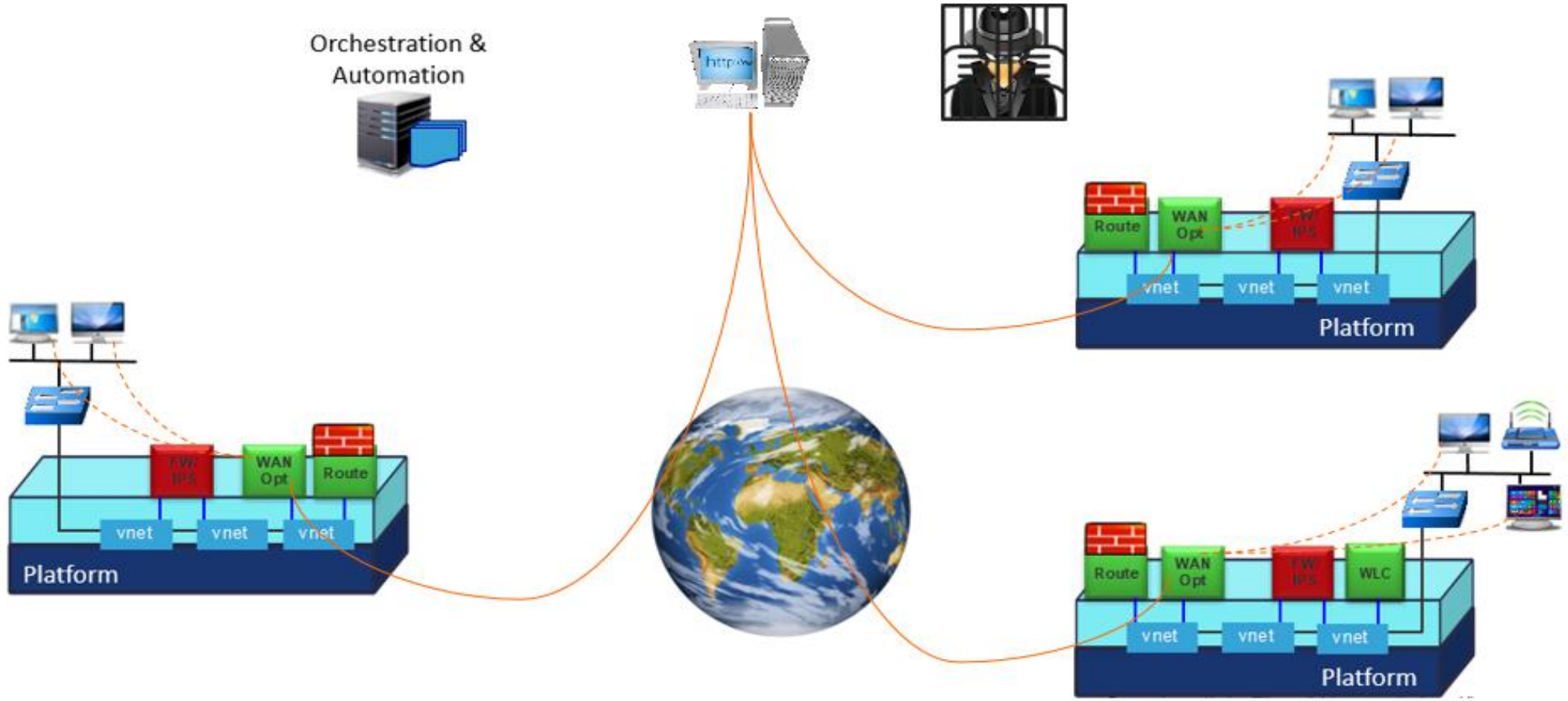
OPEX important

Upgrades, renouvellements, déplacements sur site

La solution : virtualiser les fonctions sur les sites distants

La virtualisation des services sur les sites distants

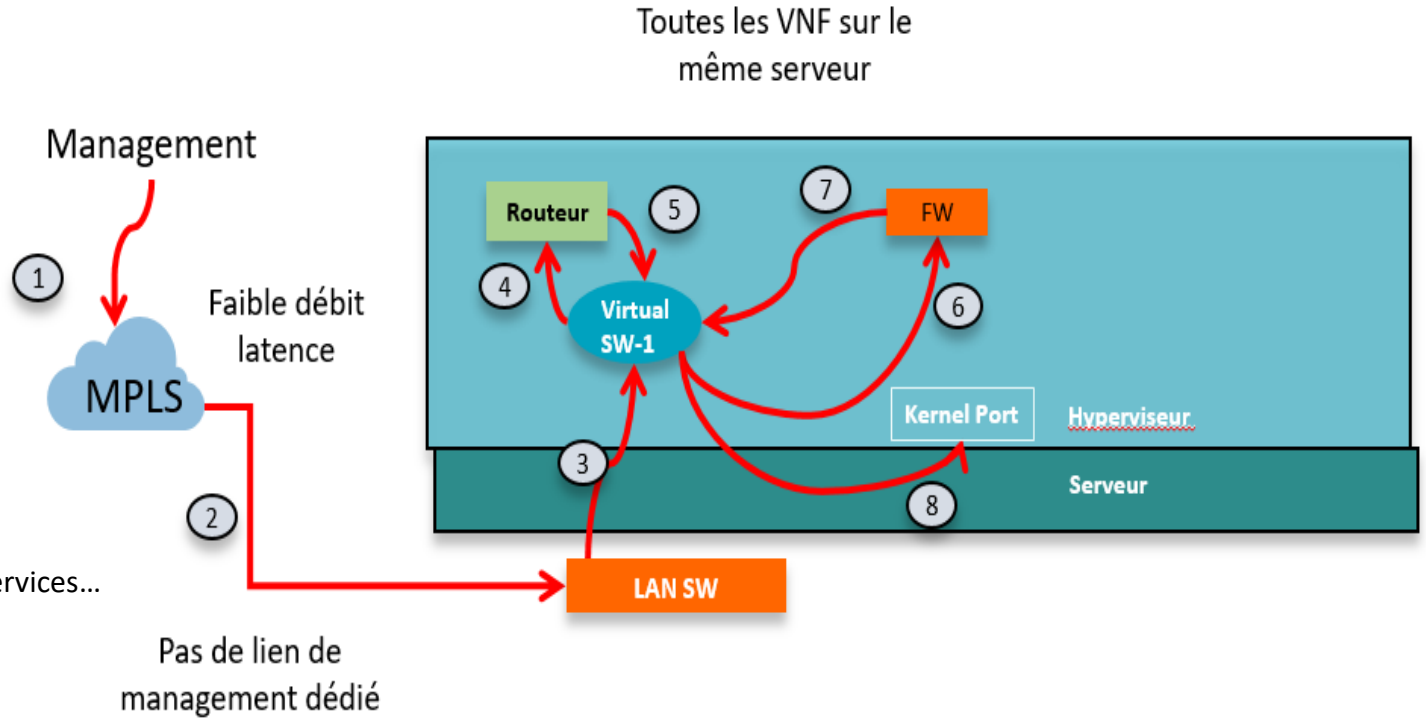
Il est possible de faire en tirant parti d'un système d'automatisation centralisé pour distribuer la politique avec une plate-forme de services réseau virtualisés



La Virtualisation sur les sites distants Spécificités

- Format du serveur (Encombrement, bruit, durcissement…)
- Connectivité (LTE, DSL…?)
- Simplicité de déploiement (ZTP)
- Ouverture à de nombreuses VNF
- Performance
- Management
- Intégration dans l'écosystème réseau

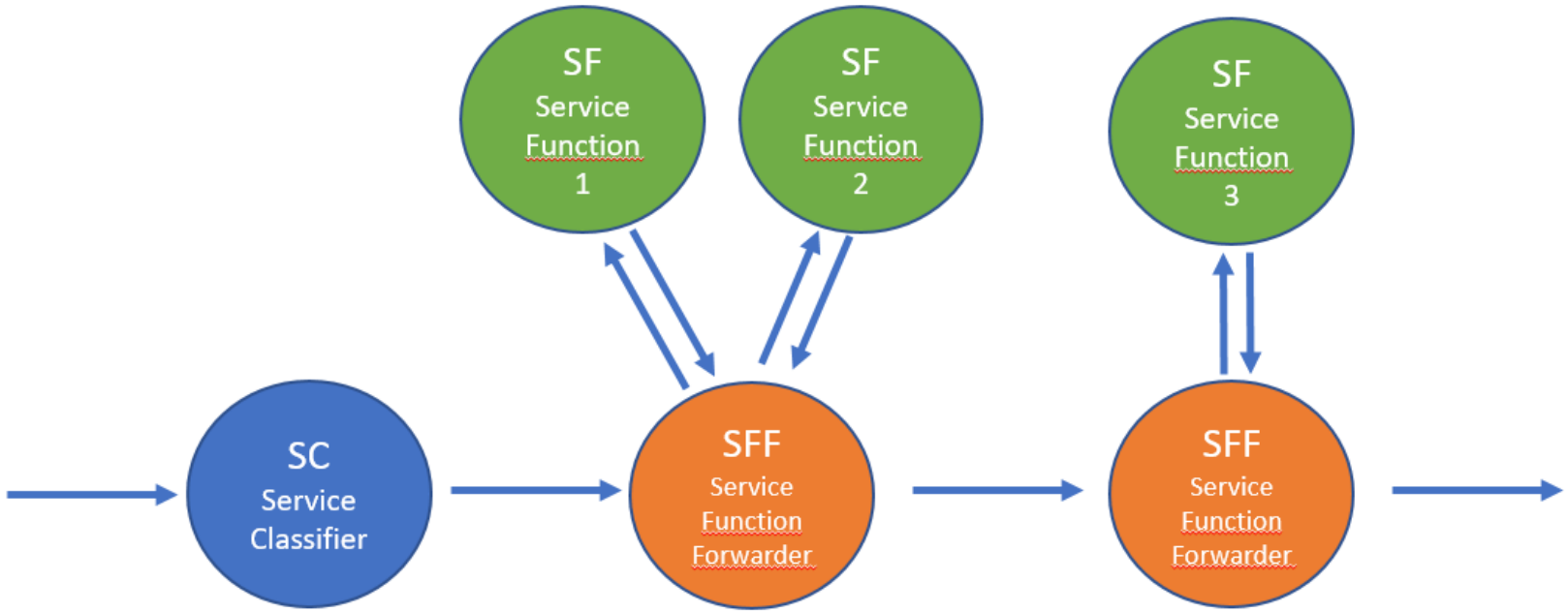
… et bien sûr le besoin d'optimiser le chaînage entre tous les services…



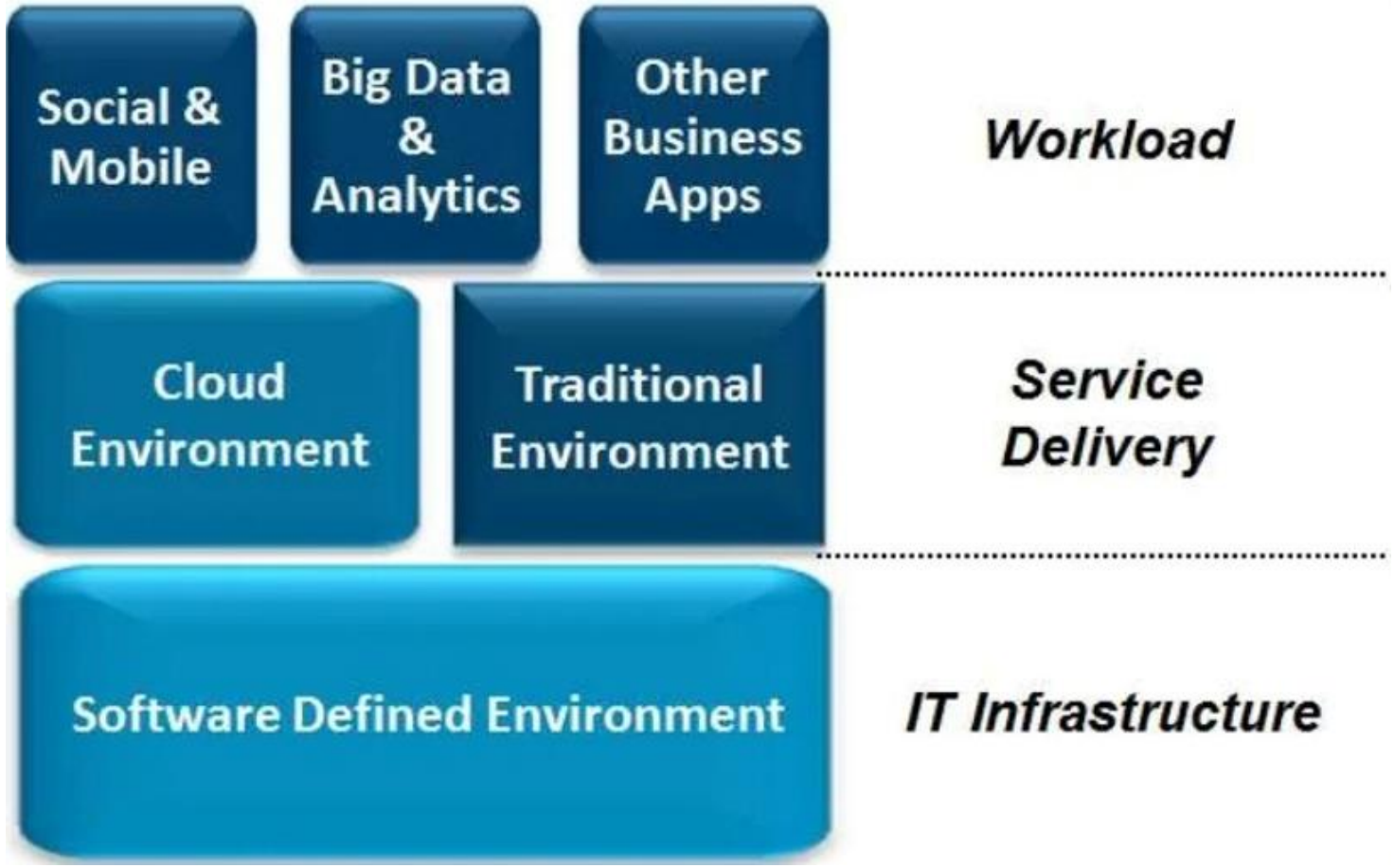
PARTIE 1

NSH – Network Service Header

- NSH en développement pour le service chaining
- IETF WG sfc (Service Function Chaining)
- Problématique et Architecture définis dans RFC 7498 et 7665
- Objectif : mieux articuler les fonctions réseau entre elles (échange de Metadata)
- Laisse la liberté au mécanismes de communication réseau entre VNF (native, GRE, VXLAN…)

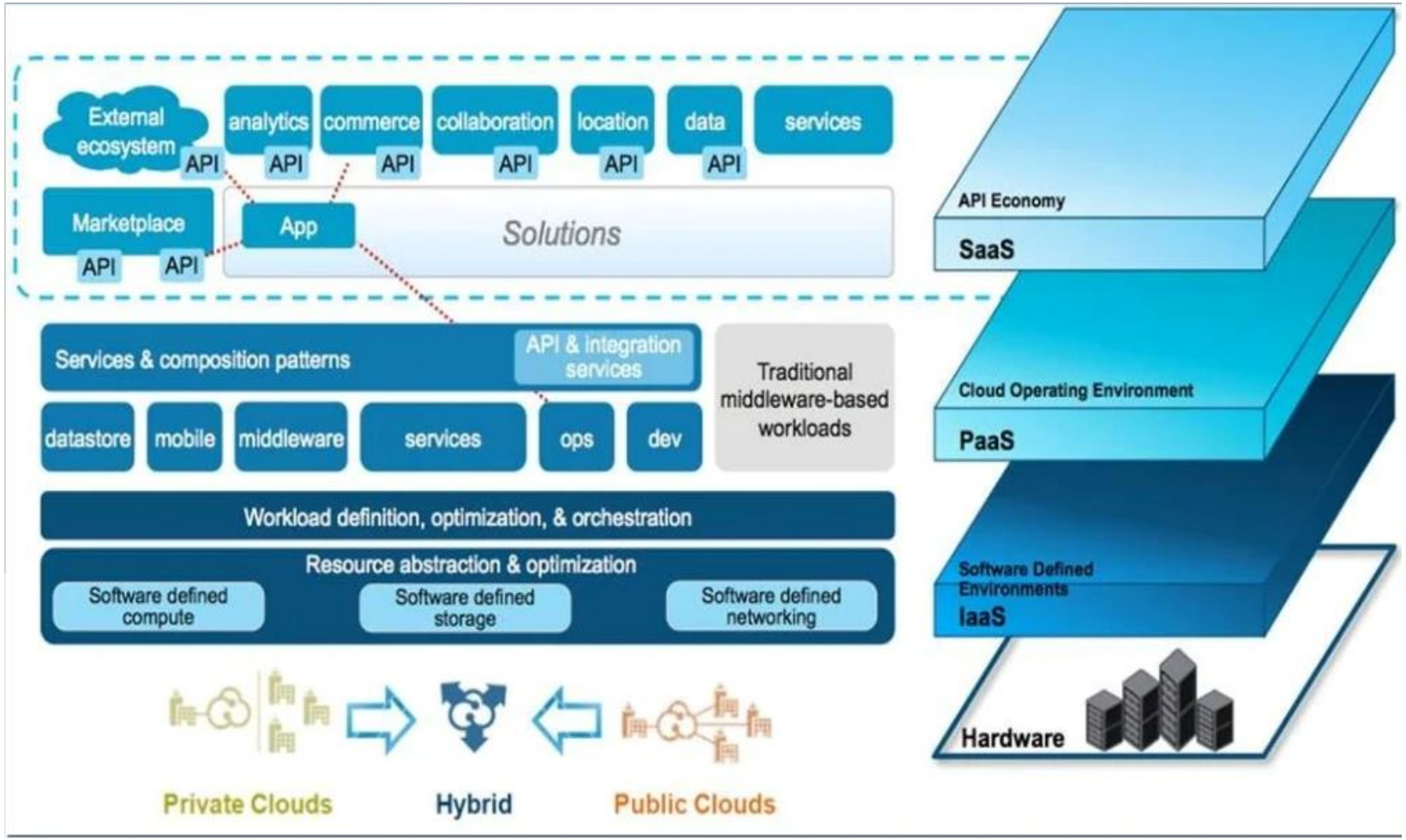


Software Defined Environement (SDE)



PARTIE 1

Cloud computing IaaS/PaaS/SaaS et Software Defined Environement (SDE)



CHAPITRE 2

Présenter la IAC et API

Ce que vous allez apprendre dans ce chapitre :

- Comprendre le concept du cloud networking

6 heures

CHAPITRE 1

Présenter la IAC et API

1. Infrastructure As a Code
2. Programmabilité des réseaux _ API

Augmentation de l'Automatisation

De nos jours, l'automatisation est partout, des caisses en libre-service disponibles dans les magasins aux contrôles environnementaux dans les bâtiments, en passant par les voitures et les avions autonomes.

Voici quelques avantages de l'automatisation :

- La productivité est donc supérieure, car les machines peuvent fonctionner 24 heures sur 24, sans aucune pause.
- Les Machines fournissent un produit plus uniforme.
- L'automatisation permet la collection d'immenses volumes de données qui peuvent être analysées rapidement pour fournir des informations qui aident à guider un événement ou un processus.
- Les robots sont utilisés dans des conditions dangereuses comme l'exploitation minière, la lutte contre les incendies et le nettoyage des accidents industriels. Cela réduit le risque pour l'homme.
- Dans certaines circonstances, les appareils intelligents peuvent modifier leur comportement pour réduire la consommation d'énergie, poser un diagnostic médical et améliorer la sécurité de conduite automobile

Format de données (JSON, YAML, XML)

- **Le concept des formats de données**

- Les formats de données sont simplement un moyen de stocker et d'échanger des données dans un format structuré. Un de ces formats est appelé Hypertext Markup Language (HTML). HTML est un langage de balisage standard pour décrire la structure des pages Web.
- Voici quelques formats de données courants utilisés dans de nombreuses applications, y comprennent l'automatisation du réseau et la programmabilité :
  - Notation d'objet JavaScript (JSON)
  - Langage de balisage extensible (XML) (Extensible Markup Language)
  - YAML n'est pas un langage de balisage (YAML)

- **Règles de format des données**

Les formats de données ont des règles et une structure similaires à celles que nous avons avec la programmation et les langages écrits. Chaque format de données aura des caractéristiques spécifiques :

- Syntaxe, qui inclut les types de parenthèses utilisés, tels que \ [\], ( ), { }, l'utilisation d'espaces blancs ou l'indentation, les guillemets, les virgules, etc.
- Comment les objets sont représentés, comme les caractères, les chaînes, les listes et les tableaux.
- Comment les paires clé / valeur sont représentées. La clé se trouve généralement sur le côté gauche et identifie ou décrit les données. La valeur à droite correspond aux données elles-mêmes et peut être un caractère, une chaîne, un nombre, une liste ou un autre type de données.

```
{"message": "success","timestamp": 1560789260,"iss_position": {"latitude": "25.9990","longitude": "-132.6992"}}
```

Format de données (JSON, YAML, XML)

Format JSON

```
{
 "message": "success",
          "timestamp": 1560789260,
          "iss_position": {
            "latitude": "25.9990",
            "longitude": "-132.6992"
          }
}
```

Format XML

```
<?xml version="1.0" encoding="UTF-8" ?>
<root>
<message>success</message>
<timestamp>1560789260</timestamp>
<iss_position>
   <latitude>25.9990</latitude>
   <longitude>-132.6992</longitude>
</iss_position>
</root>
```

Format YAML

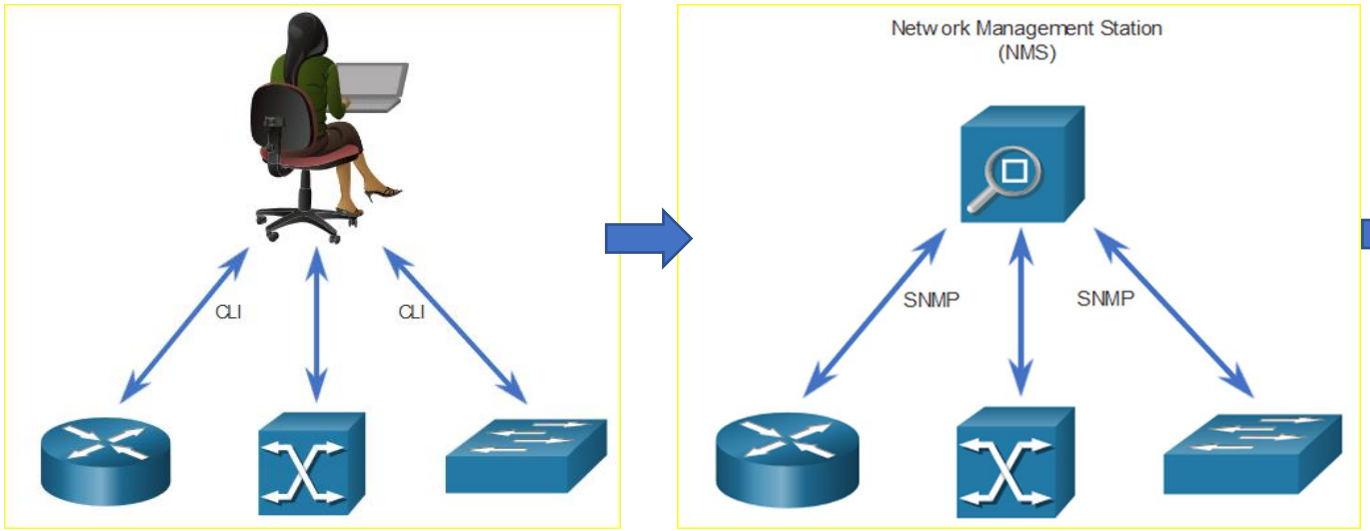
```
message: succes
timestamp: 1560789260
iss_position:
        latitude: '25.9990'
        longitude: '-132.6992'
```

PARTIE 1

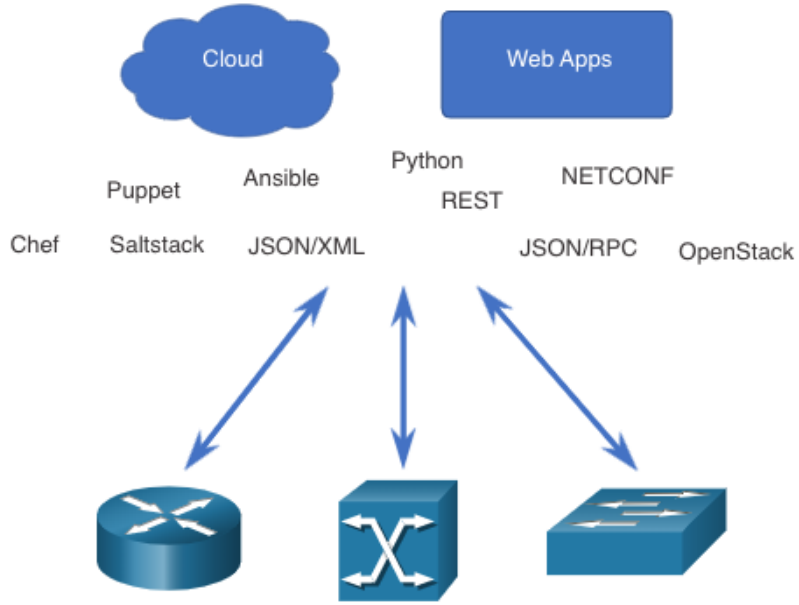
Automatisation du Réseau

Nous nous éloignons rapidement d'un monde où un administrateur réseau gère quelques dizaines de périphériques réseau, vers un monde où ils déploient et gèrent un grand nombre de périphériques réseau complexes (physiques et virtuels) à l'aide de logiciels. Cette transformation se propage rapidement à tous les endroits du réseau. Il existe de nouvelles méthodes différentes pour les administrateur de réseau pour surveiller, gérer et configurer automatiquement le réseau. Il s'agit notamment de protocoles et de technologies telles que REST, Ansible, Puppet, Chef, Python, JSON, XML, etc.

Configuration Réseau Traditionnelle



Configuration Réseau Moderne



Outils de Gestion de La Configuration

Les outils de gestion de la configuration utilisent les demandes d'API RESTful pour automatiser les tâches et peuvent évoluer sur des milliers de périphériques. Voici quelques caractéristiques du réseau que les administrateurs bénéficient de l'automatisation:

- Logiciel et contrôle de version
- Attributs de périphérique tels que les noms, l'adressage et la sécurité
- Configurations de protocole
- Configuration des listes de contrôle d'accès

Les outils de gestion de la configuration incluent généralement l'automatisation et l'orchestration. L'automatisation est lorsqu'un outil exécute automatiquement une tâche sur un système. L'orchestration est l'organisation des tâches automatisées qui se traduit par un processus de coordonnées ou un flux de travail

Plusieurs outils sont disponibles pour faciliter la gestion de la configuration:

L'objectif de tous ces outils est de réduire la complexité et le temps nécessaires à la configuration et à la maintenance d'une infrastructure de réseau à grande échelle avec des centaines, même des milliers d'appareils. Ces mêmes outils peuvent également bénéficier à des réseaux plus petits.

Outils de Gestion de La Configuration

Ansible, Chef, Puppet et SaltStack sont tous livrés avec la documentation de l'API pour configurer les demandes d'API RESTful. Tous prennent en charge JSON et YAML ainsi que d'autres formats de données. Le tableau suivant présente un résumé d'une comparaison des caractéristiques principales des outils de gestion de configuration Ansible, Puppet, Chef et SaltStack.

Caractéristique	Ansible	Chef	Puppet	SaltStack
Quel langage de programmation?	Python + YAML	Ruby	Ruby	Python
Avec ou sans agent?	Sans agent	Approche reposant sur un agent	Prend en charge les deux	Prend en charge les deux
Comment les périphériques sont-ils gérés?	Tout appareil peut être «contrôleur»	Chef Master	Puppet Master	Salt Master
Qu'est-ce qui est créé par l'outil?	Guide de vente (Playbook)	Livre de recettes	Manifeste	Pilier

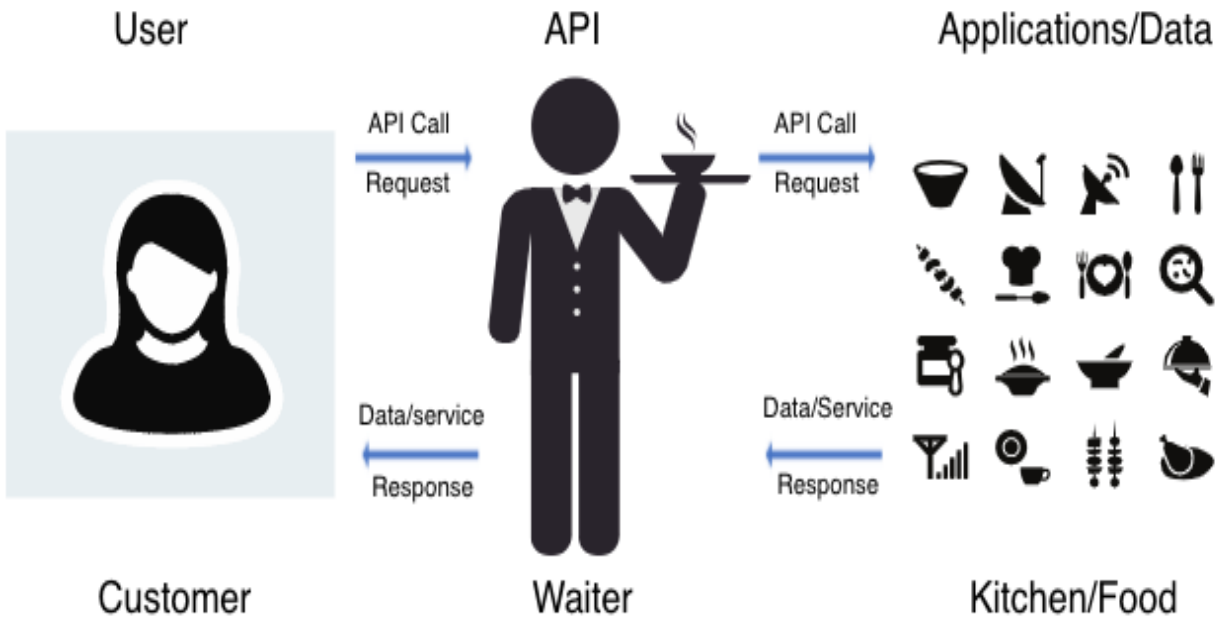
CHAPITRE 1

Présenter la IAC et API

1. Infrastructure As a Code
2. Programmabilité des réseaux _ API

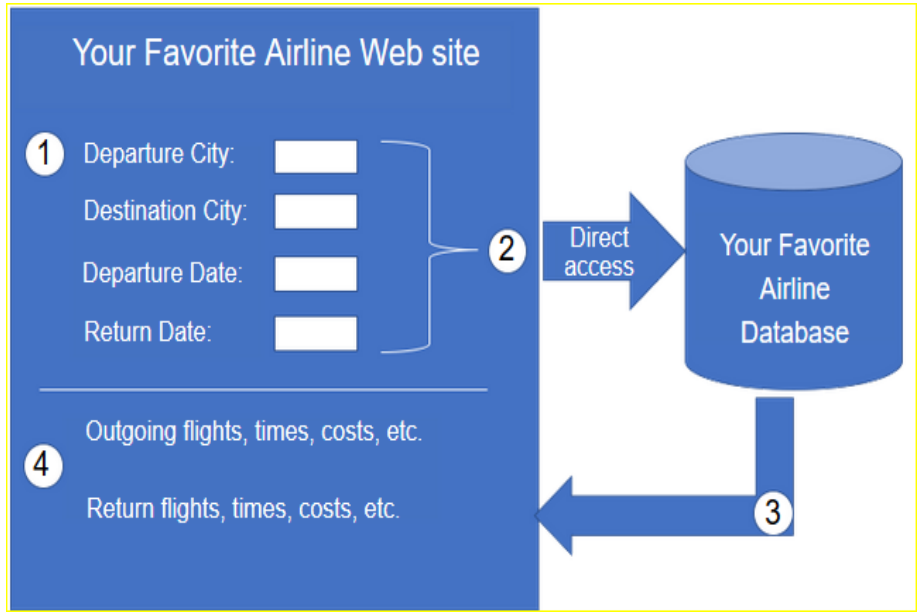
Le concept de l’ API

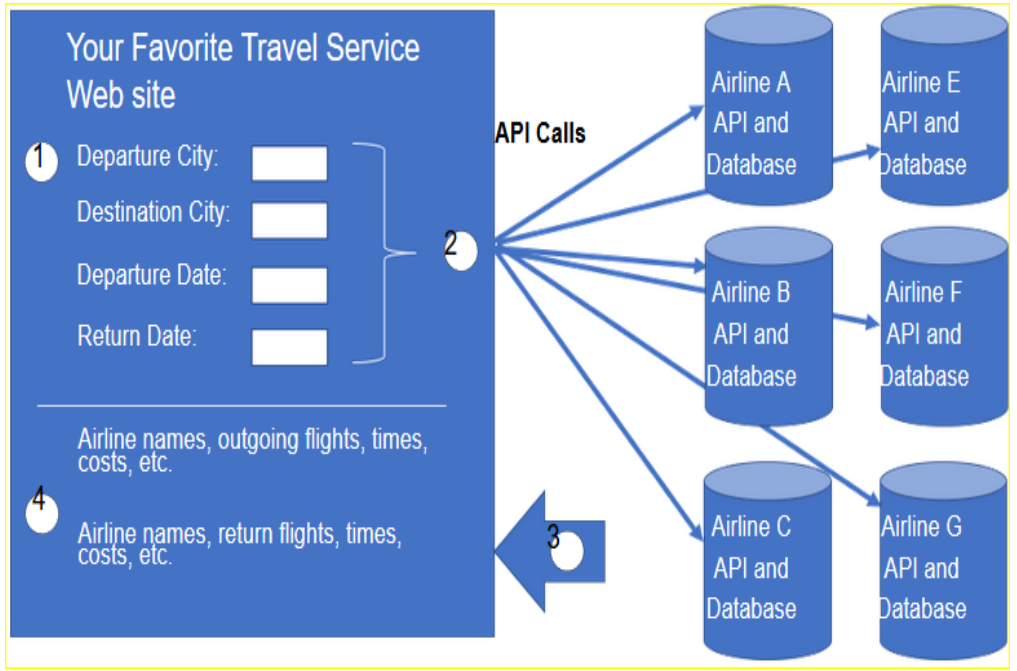
- Une API est un logiciel qui permet à d'autres applications d'accéder à ses données ou services. Il s'agit d'un ensemble de règles décrivant comment une application peut interagir avec une autre et les instructions permettant à l'interaction de se produire. L'utilisateur envoie une requête d'API à un serveur demandant des informations spécifiques et reçoit une réponse d'API en retour du serveur avec les informations demandées.
- Une API est similaire à un serveur dans un restaurant, comme illustré dans la figure suivante.



PARTIE 1

Exemple de l' API

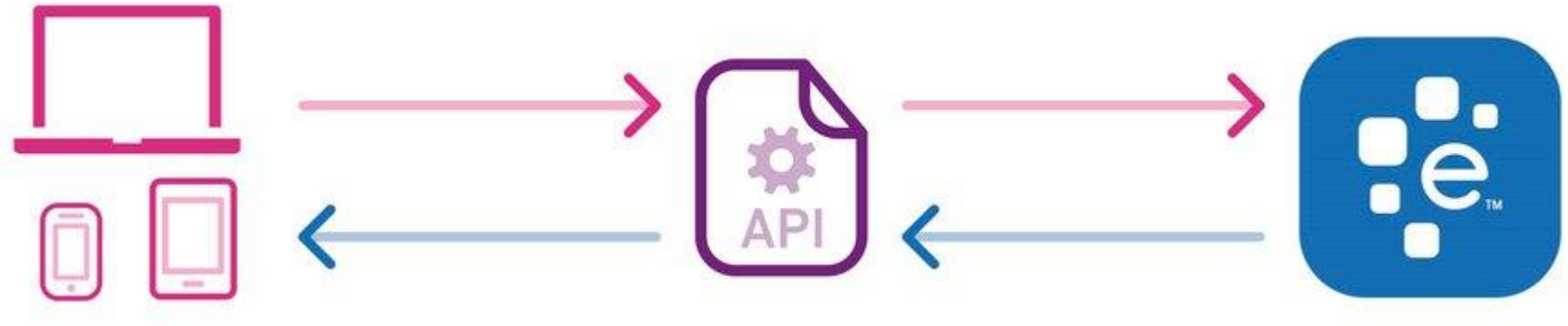




API ouverts, internes et partenaires

Une considération importante lors du développement d'une API est la distinction entre les API ouvertes, internes et partenaires:

- **API ouvertes ou API publiques -** Ces API sont disponibles au public et peuvent être utilisées sans aucune restriction. Étant donné que ces API sont publiques, de nombreux fournisseurs d'API exigent que l'utilisateur obtienne une clé ou un jeton gratuit avant d'utiliser l'API. Cela permet de contrôler le nombre de demandes d'API qu'ils reçoivent et traitent.
- **API internes ou privées** -Ce sont des API qui sont utilisées par une organisation ou une entreprise pour accéder aux données et services pour un usage interne uniquement. Un exemple d'API interne permet aux vendeurs autorisés d'accéder aux données de vente internes sur leurs périphériques mobiles.
- **API partenaires -** Ce sont des API utilisées entre une entreprise et ses partenaires commerciaux ou contractures pour faciliter les échanges entre eux. Le partenaire commercial doit disposer d'une licence ou d'une autre forme d'autorisation pour utiliser l'API. Un service de voyage utilisant l'API d'une compagnie aérienne est un exemple d'API partenaire.



Types d'API de service Web

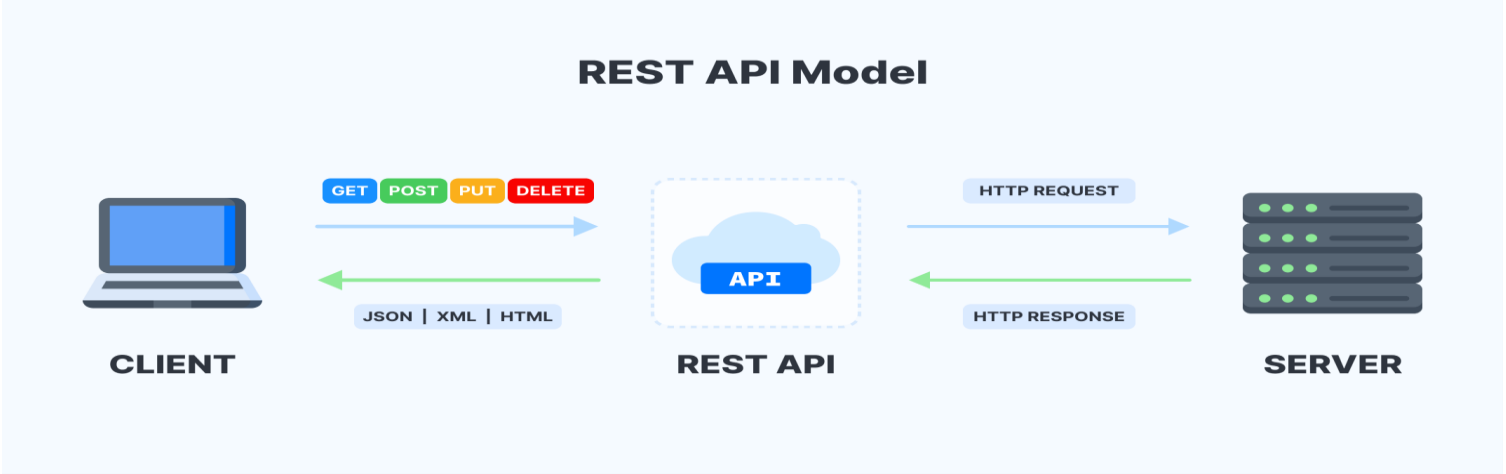
Un service Web est un service disponible sur internet via le World Wide Web. Il existe quatre types d'API de service Web:

- Protocole d'accès aux objets simples **(SOAP)**
- Transfert d'état représentatif **(REST)**
- Langage de balisage extensible-Appel de procédure à distance **(XML-RPC)**
- JavaScript notation d'objet-Appel de procédure à distance **(JSON-RPC)**

Caractéristique	SOAP	REST	XML-RPC	JSON-RPC
Format de données	XML	JSON, XML, YAML et autres	XML	JSON
Première publication	1998	2000	1998	2005
Forces	Bien établi	Formatage flexible et le plus largement utilisé	Bien établi, simplicité	Simplicité

API REST/RESTful

- Les navigateurs Web utilisent HTTP ou HTTPS pour demander (GET) une page Web. S'ils sont correctement demandés (code d'état HTTP 200), les serveurs Web répondent aux demandes GET avec une page Web codée HTML.
- En termes simples, une API REST est une API qui fonctionne au-dessus du protocole HTTP. Il définit un ensemble de fonctions que les développeurs peuvent utiliser pour effectuer des requêtes et recevoir des réponses via le protocole HTTP tel que GET et POST.
- La conformité aux contraintes de l'architecture REST est généralement appelée «RESTful». Une API peut être considérée comme «RESTful» si elle possède les fonctionnalités suivantes:
  - **Client / serveur** - Le client gère l'extrémité avant et le serveur gère l'extrémité arrière. L'un ou l'autre peut être remplacé indépendamment de l'autre.
  - **Apatride** - Aucune donnée client n'est stockée sur le serveur entre les requêtes. L'état de session est stocké sur le client.
  - **Cacheable** - Les clients peuvent mettre en cache les réponses pour améliorer les performances.

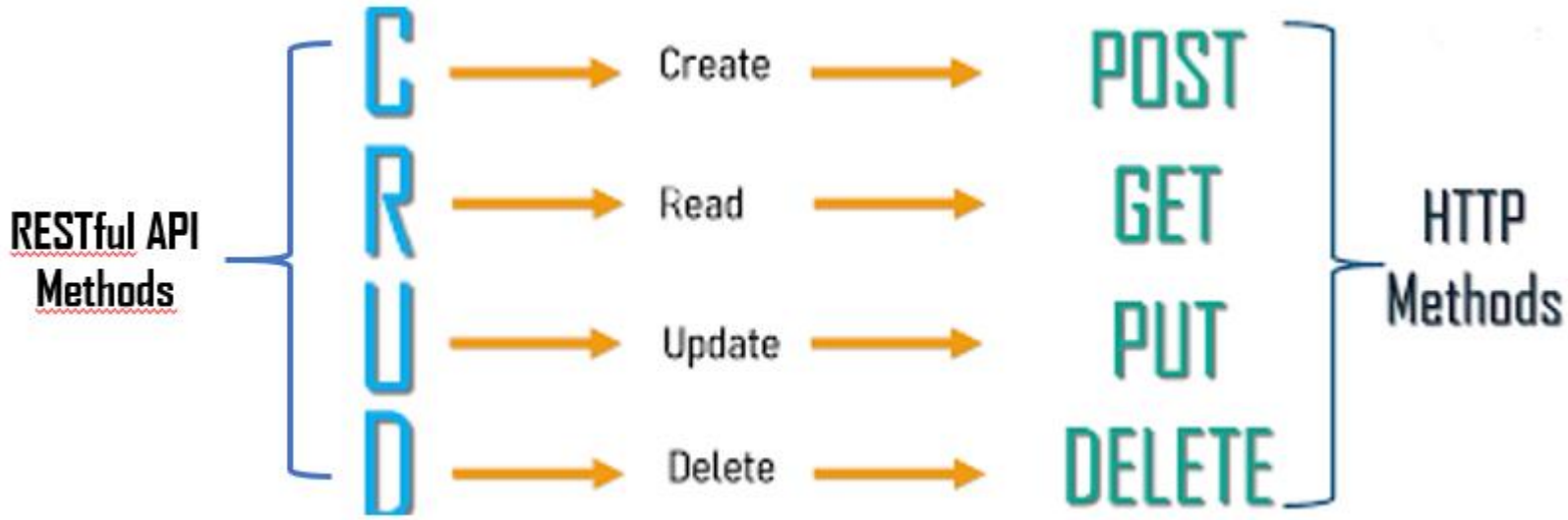


Mise en œuvre RESTful

Un service Web RESTful est implémenté à l'aide de HTTP. Il s'agit d'une collection de ressources avec quatre aspects définis:

- L'identificateur de ressource uniforme de base (URI) pour le service Web, tel que http://example.com/resources.
- Format de données pris en charge par le service Web. Il s'agit souvent de JSON, YAML ou XML, mais il peut s'agir de tout autre format de données qui constitue une norme hypertexte valide.
- Ensemble d'opérations prises en charge par le service Web à l'aide de méthodes HTTP.
- L'API doit être basée sur l'hypertexte.

Les API RESTful utilisent des méthodes HTTP courantes.

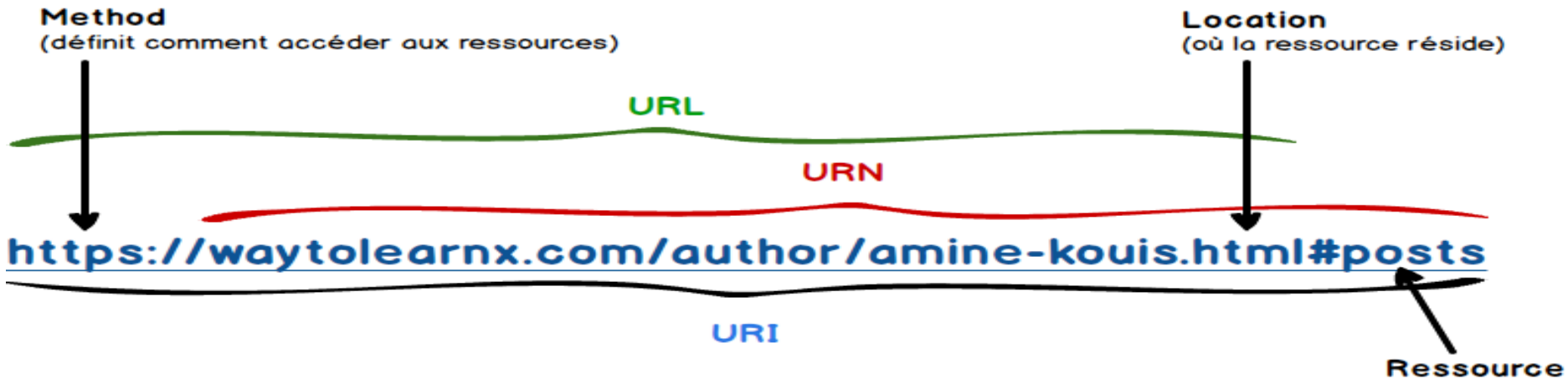


URI, URN, et URL

Les ressources Web et les services Web tels que les API RESTful sont identifiés à l'aide d'un URI.

Un **URI** est une chaîne de caractères qui identifie une ressource de réseau spécifique. Un URI a deux spécialisations:

- **Nom de ressource uniforme (URN)** - identifie uniquement l'espace de noms de la ressource (page Web, document, image, etc.) sans référence au protocole.
- **Localisateur de ressources uniforme (URL)** - définit l'emplacement réseau d'une ressource spécifique. Les URL HTTP ou HTTPS sont généralement utilisées avec les navigateurs Web. Des protocoles tels que FTP, SFTP, SSH et autres peuvent utiliser une URL. Une URL utilisant SFTP peut ressembler à: sftp: //sftp.example.com.

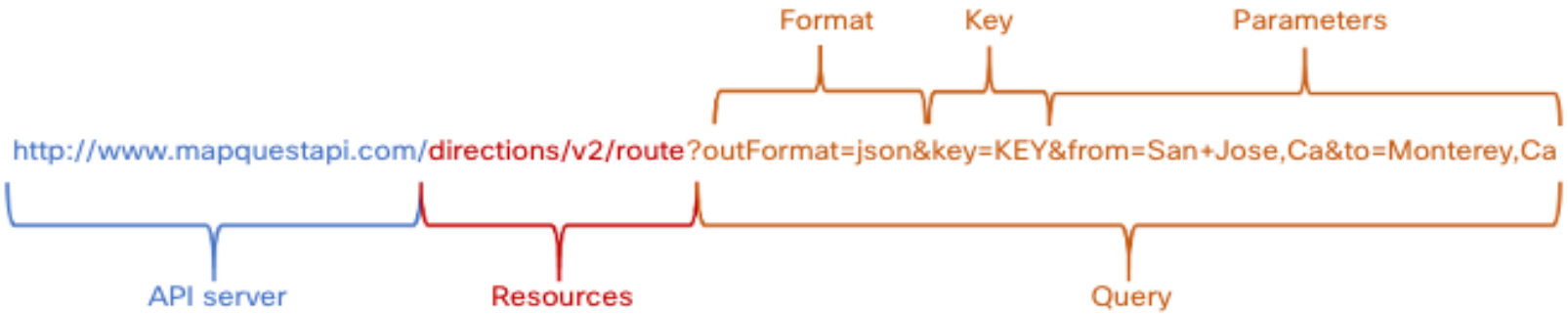


Anatomie d'une demande RESTful

Dans un service Web RESTful, une demande adressée à l'URI d'une ressource provoquera une réponse. La réponse sera une charge utile généralement formatée en JSON, mais pourrait être HTML, XML ou un autre format. La figure indique l'URI de l'API directions MapQuest. La demande d'API est pour les directions de San Jose, Californie à Monterey, Californie.

Voici les différentes parties de la demande d'API:

- **Serveur API** - Il s'agit de l'URL du serveur qui répond aux demandes REST. Dans cet exemple, il s'agit du serveur API MapQuest.
- **Ressources** - Spécifie l'API qui est demandée Dans cet exemple, il s'agit de l'API directions MapQuest.
- **Requête** - Spécifie le format de données et les informations que le client demande au service API. Les requêtes peuvent inclure:
  - **Format** – Il s'agit généralement de JSON mais peut être YAML ou XML. Dans cet exemple, JSON est demandé.
  - **Clé** - La clé est pour l'autorisation, si nécessaire. MapQuest nécessite une clé pour son API de directions. Dans l'URI ci-dessus, vous devez remplacer «KEY» par une clé valide pour soumettre une demande valide.
  - **Paramètres** - Les paramètres sont utilisés pour envoyer des informations relatives à la demande. Dans cet exemple, les paramètres de requête incluent des informations sur les directions dont l'API a besoin pour qu'elle sache les directions pour retourner: "from = San + Jose, Ca" et "to = Monterey, Ca".



Remarque: Recherchez l'URL sur internet pour obtenir une clé MapQuest. Utilisez les paramètres de recherche: developer.mapquest.

PARTIE 1

Les Application d'API RESTful

- De nombreux sites Web et applications utilisent des API pour accéder aux informations et fournir des services à leurs clients.
- Certaines demandes d'API RESTful peuvent être effectuées en tapant l'URI à partir d'un navigateur Web. Dans cet exemple, il s'agit de l'API directions MapQuest. Une demande d'API RESTful peut également être effectuée par d'autres moyens.
  - **Le web site developpeur**: Les développeurs gèrent souvent des sites Web qui contiennent des informations sur l'API, des informations sur les paramètres et des exemples d'utilisation. Ces sites peuvent également permettre à l'utilisateur d'effectuer la demande d'API dans la page Web du développeur en entrant les paramètres et d'autres informations.
  - **Postman**: Postman est une application pour tester et utiliser les API REST. Il contient tout ce qui est nécessaire pour construire et envoyer des demandes d'API REST, y compris la saisie des paramètres de requête et des clés.
  - **Python**: Les API peuvent également être appelées à partir d'un programme Python. Cela permet une automatisation, une personnalisation et une intégration d'applications possibles de l'API.
  - **Systèmes D'exploitation Réseau**: À l'aide de protocoles tels que NETCONF (NET CONFiguration) et RESTCONF, les systèmes d'exploitation de réseau commencent à fournir une méthode alternative pour la configuration, la surveillance et la gestion.

PARTIE 2

Utiliser le Software Defined Network (SDN)

Dans ce module, vous allez :

- Être en mesure de comprendre le concept du cloud networking
- Être en mesure de maitriser les notions de base de la virtualisation des réseaux

22 heures

CHAPITRE 1

Comprendre les Concepts SDN

Ce que vous allez apprendre dans ce chapitre :

- Fonctionnement et principe de la technologie SDN

8 heures

CHAPITRE 1

Définir la technologie SDN

1. Présentation de la technologie SDN
2. Le SDN vs le réseautage traditionnel
3. Le SDN vs NFV

PARTIE 2

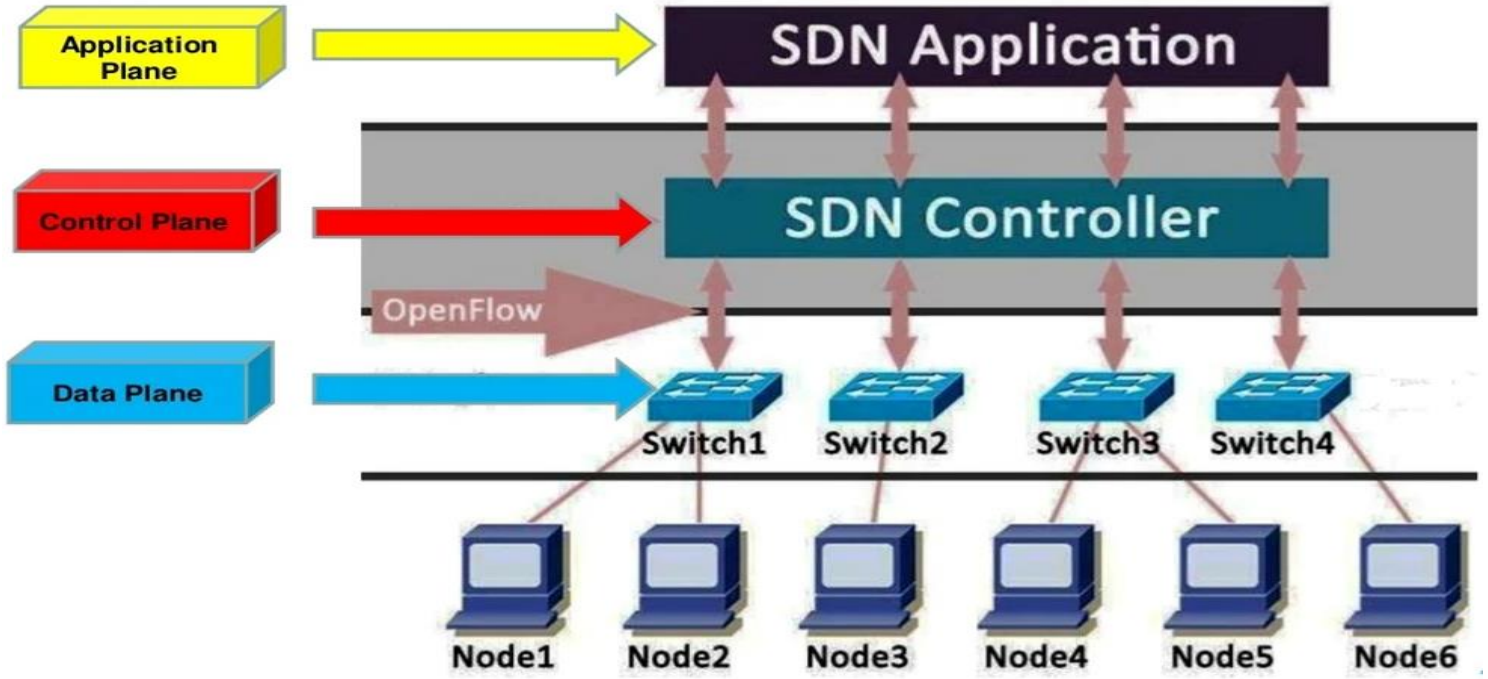
SDN (Software-Defined Networking)

- Une architecture de réseau qui virtualise le réseau, offrant une nouvelle approche de l'administration et de la gestion du réseau qui vise à simplifier et à rationaliser le processus d'administration.
- SDN est un nouveau paradigme d'architecture réseau où le plan de contrôle est totalement découplé du plan de données.

PARTIE 2

La technologie SDN

- SDN (Software-Defined Networking) est une nouvelle architecture de réseau qui comprenait différentes technologies de réseau pour construire des réseaux flexibles, évolutifs, agiles et faciles à gérer.
- Avec sa nouvelle vue, SDN découple le réseau en deux plans en tant que plan de contrôle et plan de données. Cela fournit un contrôle central du réseau et une meilleure expérience de transfert.
- De plus, SDN apporte une capacité de programmabilité aux réseaux.



Concept SDN

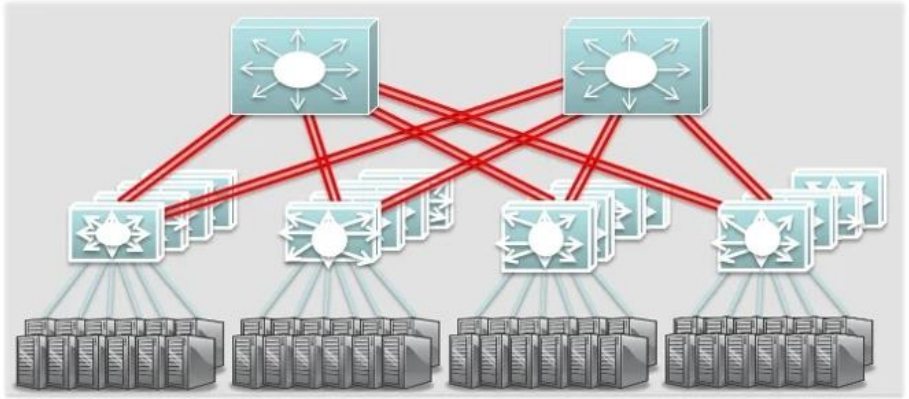
- En déplaçant le plan de contrôle dans la partie logicielle permet un accès et une administration dynamic. L'administrateur réseau peut adapter le trafic depuis une console centrale sans avoir à configurer les équipements individuellement. L'administrateur peut changer n'importe quelle règle d'un équipement réseau quand nécessaire.
- Directement programmable : le contrôle du réseau est directement programmable grâce au découplage des fonctions de relayage.
- Agile : l'abstraction du contrôle du relayage permet aux administrateurs d'ajuster dynamiquement le réseau au trafic.
- Management centralisé : l'intelligence du réseau est centralisé dans un logiciel appellé SDN contrôleur, qui maintient une vue globale du réseau.
- Configuration automatique : SDN permet aux administrateurs réseaux de configurer, administrer, sécuriser et optimiser les réseaux réseaux rapidement grâce à des programmes SDN dynamiques et automatisés. Et ces programmes peuvent être développer par eux-mêmes car ils ne dépendent plus de logiciels propriétaires.
- Basé sur des standards ouverts et vendeur-indépendant : l'implémentation à travers des standards ouverts permet de simplifier l'architecture réseau car les instructions sont fournies par un ou plusieurs contrôleurs au lieu de multiple équipements propriétaires.

PARTIE 2

Benefits SDN

Ce que SDN apporte :

- Séparation du plan de contrôle et du plan de données,
- Mécanisme central de maintenance,
- Les périphériques réseau responsables uniquement du transfert,
- Matériels à usage général,
- Système d'exploitation réseau,
- De nouvelles applications au lieu de protocoles,
- Nouveau protocole, Open Flow, NETCONF etc.
- Diminuer les CAPEX et les coûts d'exploitation,
- Fiabilité et sécurité accrues,
- Meilleur dépannage,
- Réseau entièrement contrôlé



Cost

200,000 servers

Fanout of 20 = 10,000 switches

$5k vendor switch = $50M

$1k commodity switch = $10M

Savings in 10 data centers = $400M

Control

More flexible control

Tailor network for services

Quickly improve and innovate

PARTIE 2

Terminologie SDN

SDN : Réseau défini par logiciel. C'est un nouveau réseau architecture qui comprenait différentes technologies de réseau pour construire des réseaux flexibles, évolutifs, agiles et faciles à gérer. SDN fait ce travail en séparant les plans de contrôle et de transfert:

Plan de transfert : La couche inférieure du SDN qui est pleine de périphériques de transfert physiques ou virtuels. Plan de données.

Plan de contrôle : La couche intermédiaire du SDN qui comprend le système d'exploitation réseau et le contrôleur SDN.

Plan d'application : la couche supérieure du SDN qui comprend les applications.

Interface vers le sud : L'interface entre le contrôleur et les périphériques de transmission du plan de données.

Northbound Interface : L'interface entre le contrôleur et le plan d'application.

API : Interface Programmable d'Application. Fournit une interaction entre les systèmes et les logiciels.

Commutateur de transfert : commutateur de transfert SDN utilisé dans le plan de données

Contrôleur : Le mécanisme de contrôle central du réseau SDN qui contrôle le plan de transfert.

NFV : Virtualisation des Fonctions Réseaux. Virtualisation des différents équipements réseau physiques qualifiés avec leurs homologues

Flow : Séquence de paquet entre la source et la destination

Règles de flux : actions définies pour le flux

CHAPITRE 1

Définir la technologie SDN

1. Présentation de la technologie SDN
2. Le SDN vs le réseautage traditionnel
3. Le SDN vs NFV

PARTIE 2

Les équipements réseau traditionnels

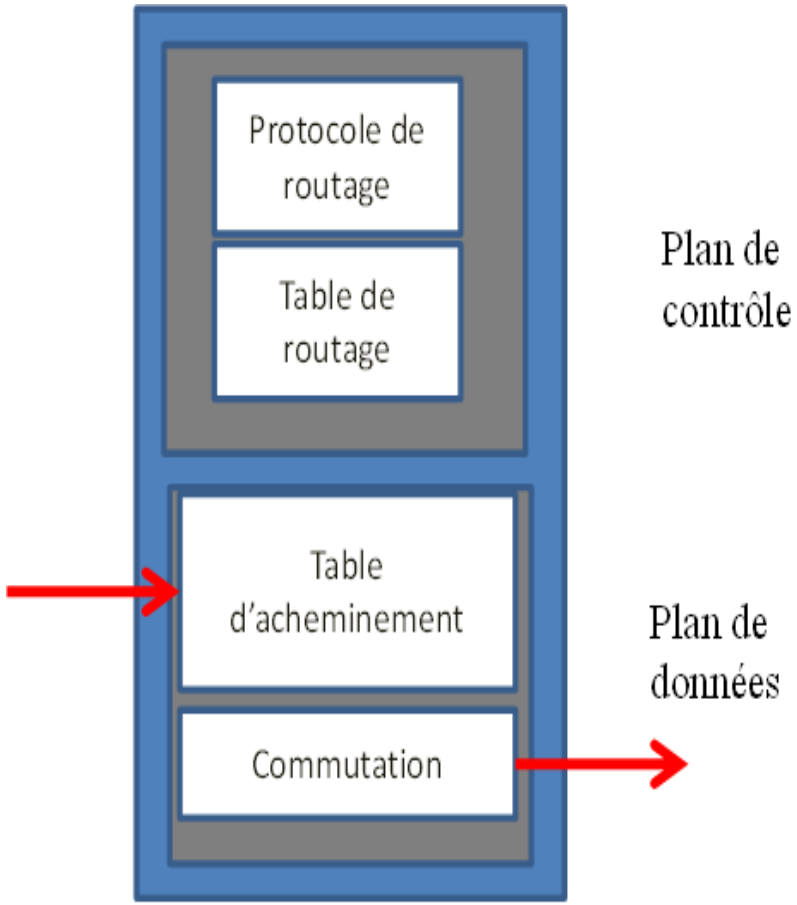
Un appareil réseau contient les plans suivants :

- **Plan de contrôle**

- Il est généralement considéré comme le cerveau d'un appareil.
- Les fonctions d'un réseau qui contrôlent le comportement du réseau
- Ex. : Quel chemin prendre pour un paquet ? Quel port rediriger un paquet? Le paquet doit-il être abandonné ?
- Les fonctions du plan de contrôle sont généralement réalisées par un logiciel tels que les protocoles de routage, le code de pare-feu, etc.

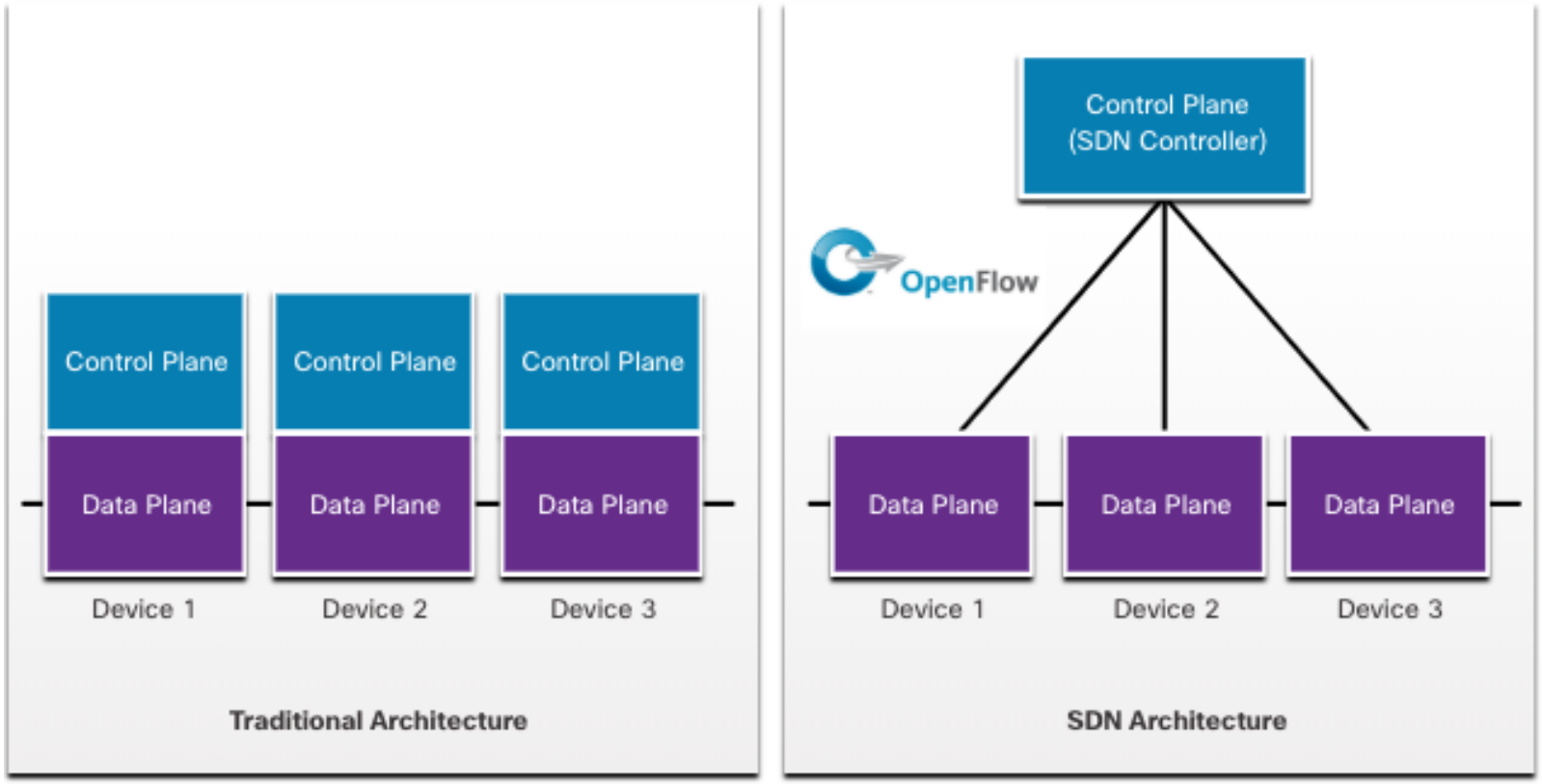
- **Plan de données**

- Également appelé plan d'acheminement
- Les fonctions d'un réseau qui transmettent ou abandonnent paquets.
- Les fonctions du plan de données sont généralement réalisées par le matériel
- **Le plan de contrôle et le plan de données sont intégrés verticalement dans les équipements réseau traditionnels**



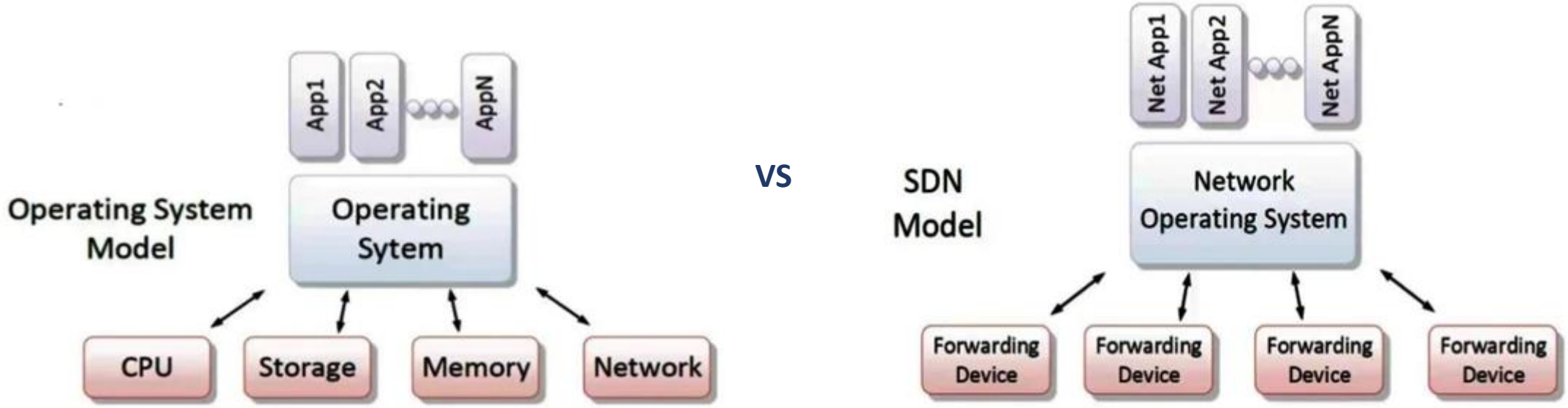
PARTIE 2

Architectures traditionnelles et SDN



PARTIE 2

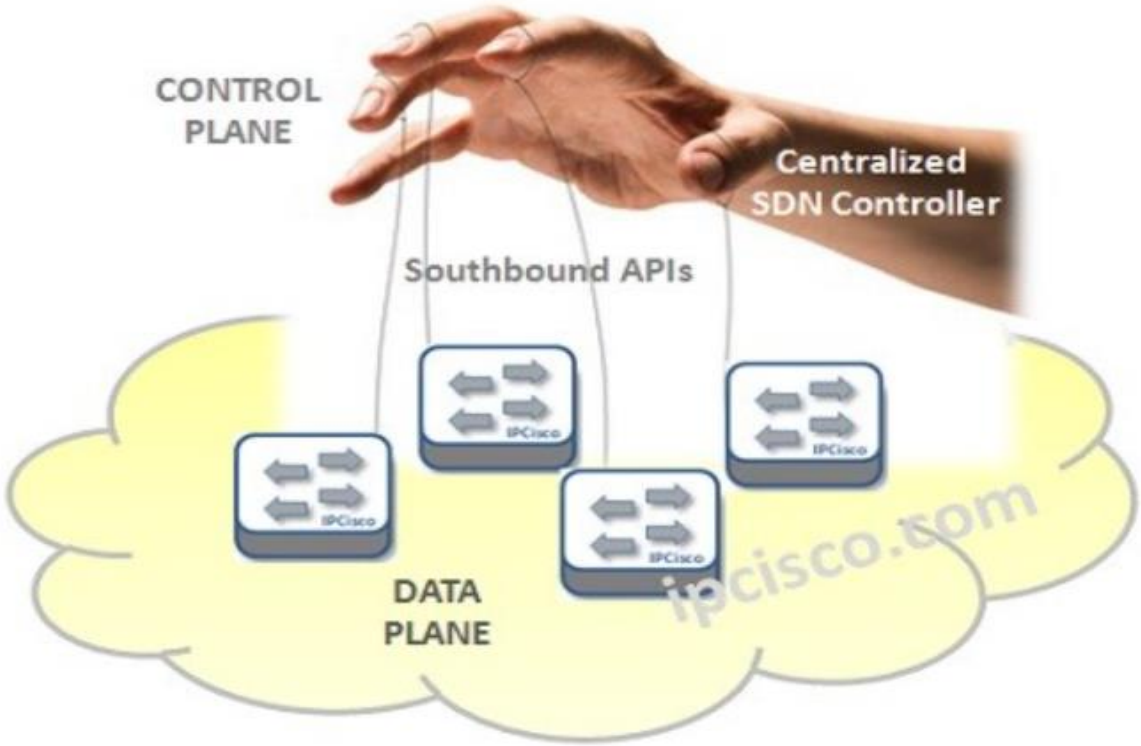
Modèle de système d'exploitation et SDN



PARTIE 2

Gestion Centralisée

- Le découplage des plans de contrôle et de données fournira une gestion centralisée. Le plan de contrôle qui gère le réseau sera au sommet de l'infrastructure réseau. Il décide et l'infrastructure ci-dessous le fera. Ainsi, avec ce mécanisme, la transmission sera également très efficace.



CHAPITRE 1

Définir la technologie SDN

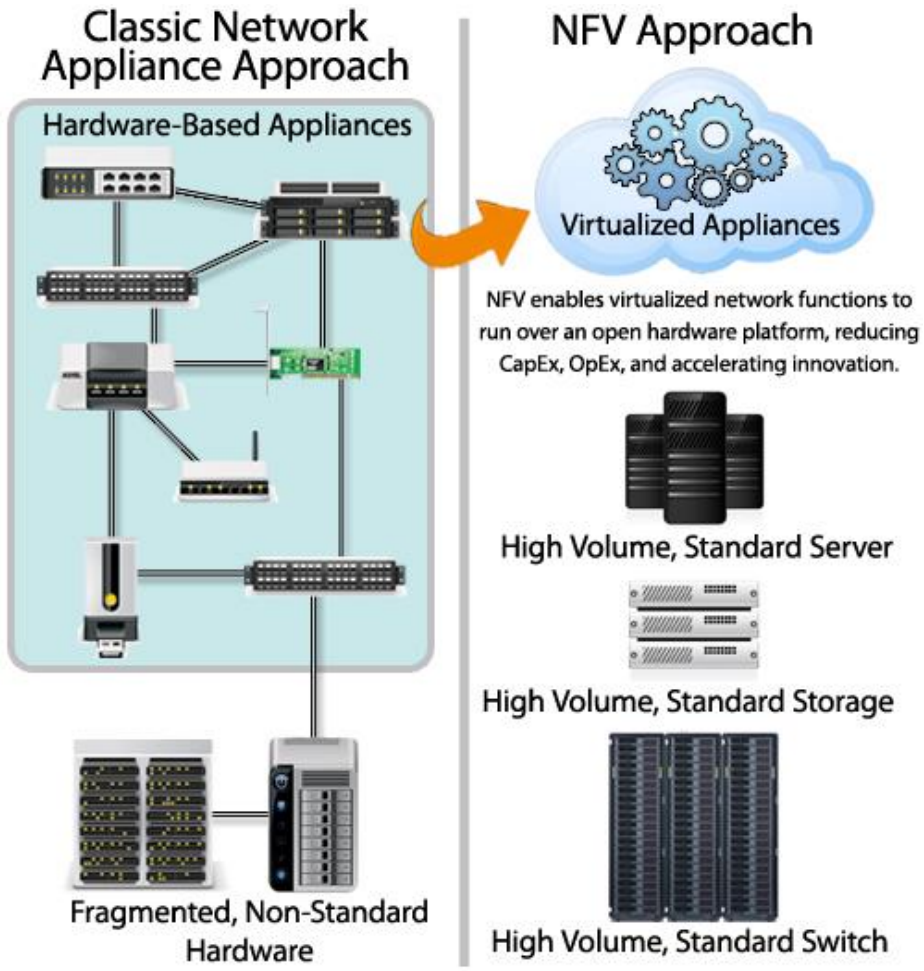
1. Présentation de la technologie SDN
2. Le SDN vs le réseautage traditionnel
3. Le SDN vs NFV

PARTIE 2

La technologie NFV

la technologie NFV fait exactement ce qu'elle désigne et virtualise les fonctions réseau telles que les ADC (contrôleurs de distribution d'applications) et les pare-feu applicatifs Web. La virtualisation des fonctions réseau ne nécessite pas de matériel propriétaire physique et permet au réseau d'exploiter pleinement la technologie de datacenter virtualisé.

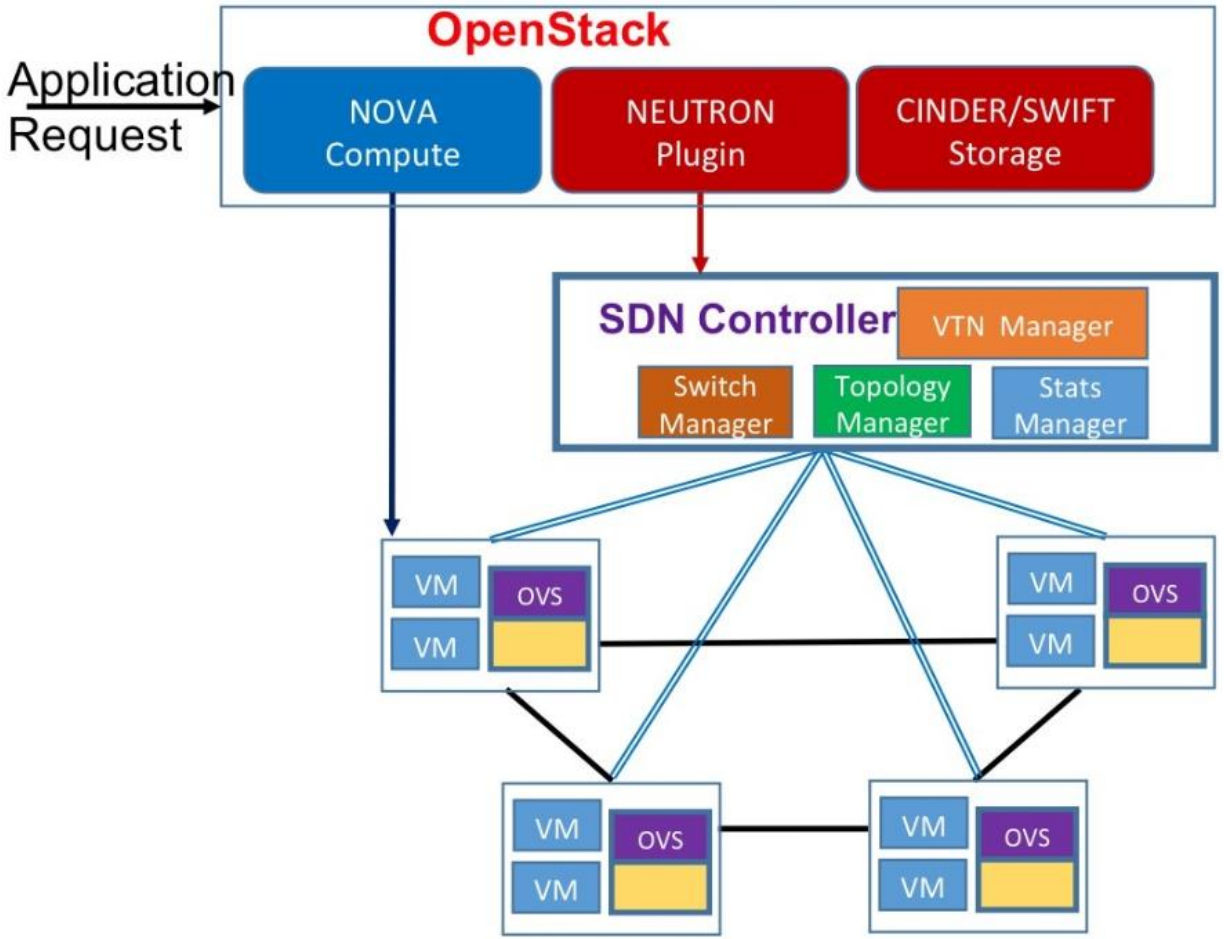
Le principe fondamental du NFV consiste à virtualiser les services réseaux pour se débarrasser des matériels dédiés. Généralement, les déploiements NFV utilisent des serveurs standards pour faire tourner des logiciels de services réseaux anciennement basés sur le matériel. Ces services basés sur le logiciel protent le nom de services de virtualisation des fonctions réseaux ou Virtual Network Functions (VNF). Ils fonctionnent dans un environnement NFV. Ces services VNF incluent le routage, les fonctions pare-feu, l'équilibrage de charge, l'accélération WAN et le cryptage.



Contrôleur SDN

- **OpenStack**
- OpenStack est une plateforme open-source pour orchestrer et maintenir les clouds.

- Cette approche repose sur une plate-forme d'orchestration et de virtualisation pour créer des environnements cloud évolutifs et mettre en œuvre une solution IaaS (infrastructure en tant que service).
- Dans le domaine des réseaux, l'orchestration correspond à l'automatisation du provisionnement de composants réseau tels que les serveurs, le stockage, les commutateurs, les routeurs et les applications.



VM : (virtual machine)

VTN: (Virtual Network Tenant) une application qui fournit un réseau virtuel multi-tenant sur un contrôleur SDN.

OVS: (Open vSwitch) nœuds et commutateurs de réseau virtuel.

PARTIE 2

CHAPITRE 1

Découvrir les architectures SDN et ces applications

Ce que vous allez apprendre dans ce chapitre :

- Fonctionnement et principe de la technologie SDN

8 heures

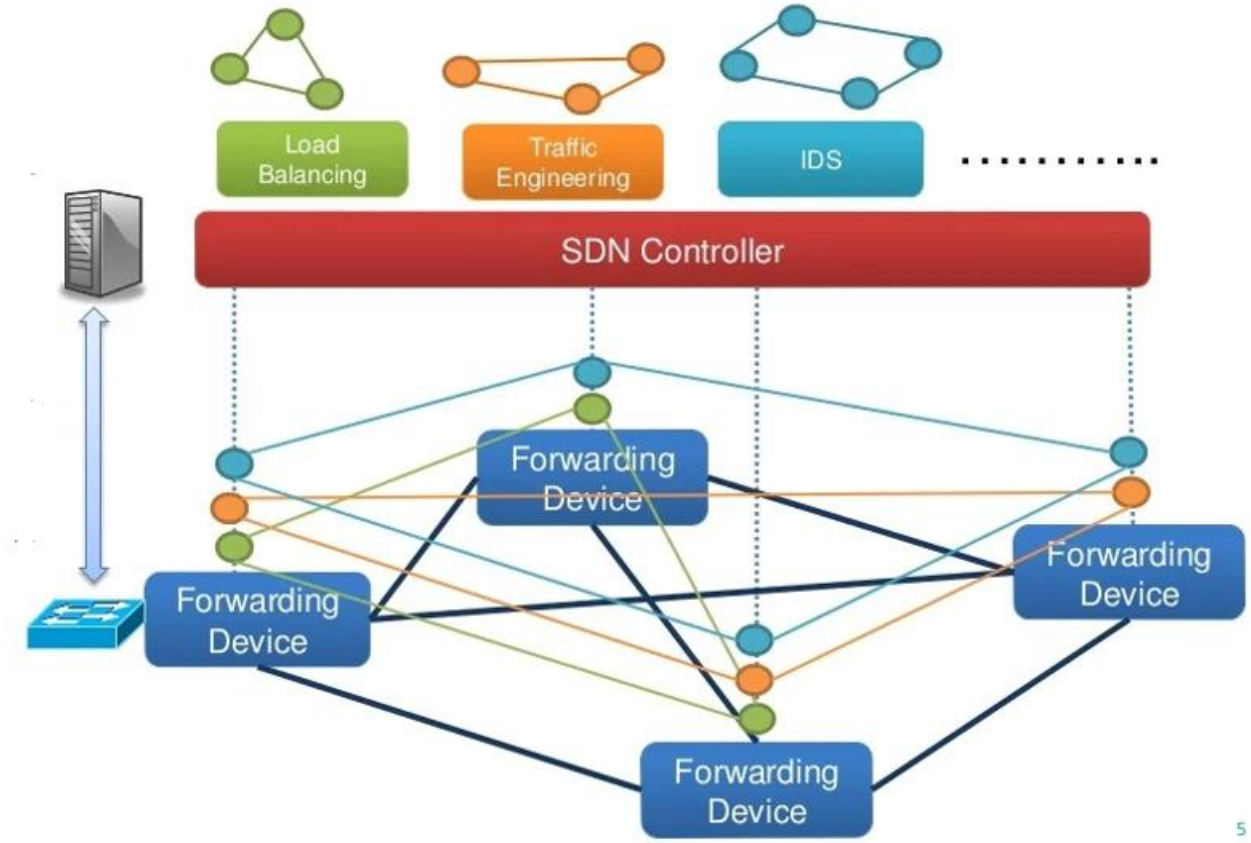
CHAPITRE 2

Découvrir les architectures SDN et ces applications

1. Fonctionnement et principe de la technologie SDN
2. Modèles de la technologie SDN
3. Les applications de la technologie SDN
4. Les solutions de la technologie SDN

PARTIE 2

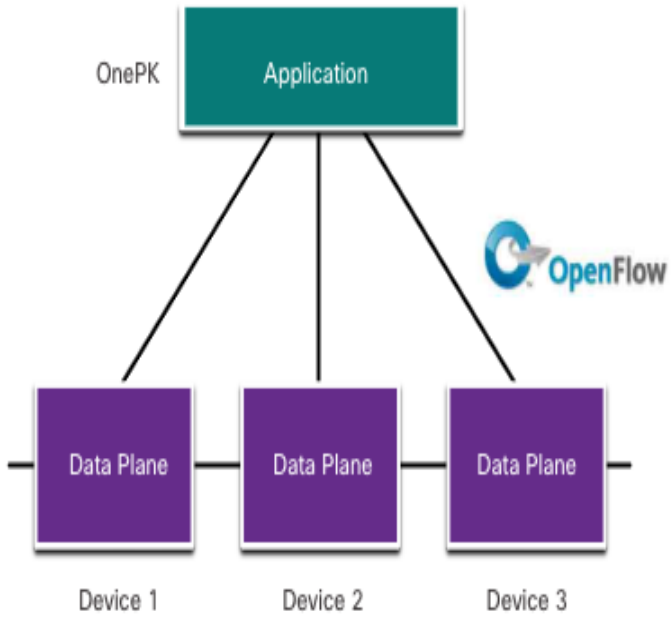
Architectures SDN



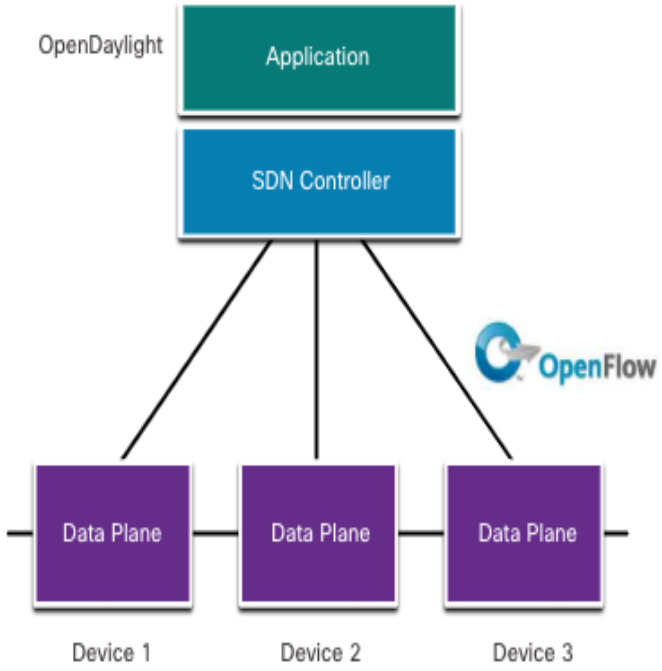
PARTIE 2

Types d'architecture SDN

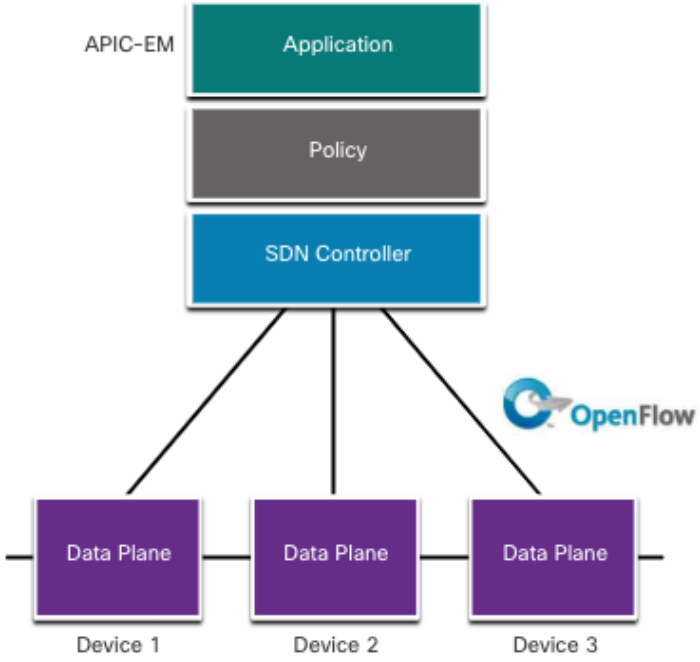
SDN basé sur les appareils



SDN basé sur un contrôleur

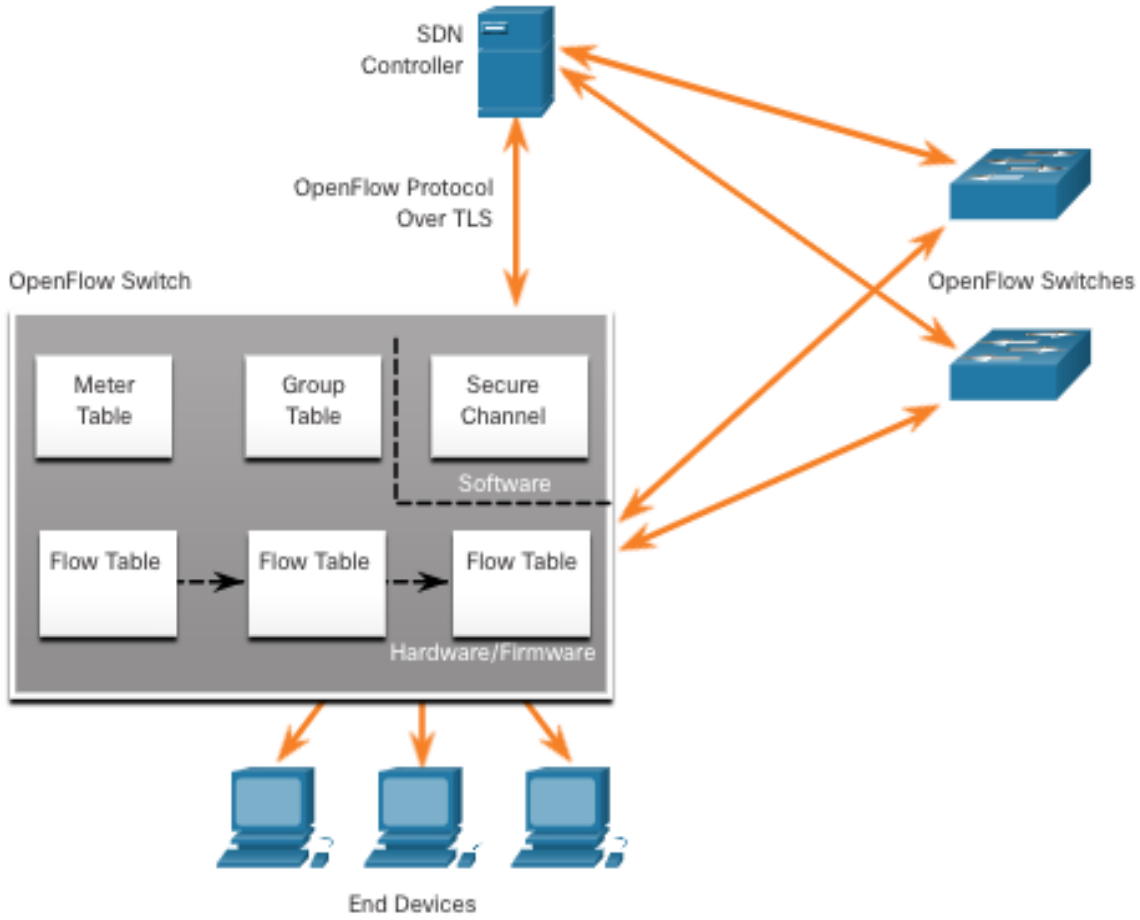


SDN basé sur des politiques



Fonctionnement du contrôleur SDN

- Le contrôleur SDN définit les flux de données entre le plan de contrôle centralisé et les plans de données sur les routeurs et les commutateurs individuels.
- Pour pouvoir traverser le réseau, chaque flux doit être approuvé par le contrôleur SDN qui vérifie que la communication est autorisée dans le cadre de la politique réseau de l'entreprise.
- Toutes les fonctions complexes sont prises en charge par le contrôleur. Le contrôleur alimente les tables de flux. Les commutateurs gèrent les tables de flux.
- Sur chaque commutateur, la gestion des flux de paquets est assurée par une série de tables (**Table des flux, Table de groupe** et **Table de comptage)** mises en œuvre au niveau du matériel ou du firmware.
- À l'échelle du commutateur, un flux est une séquence de paquets qui correspond à une entrée spécifique dans une table de flux.



PARTIE 2

CHAPITRE 2

Comprendre les Concepts SDN

1. Fonctionnement et principe de la technologie SDN
2. Modèles de la technologie SDN
3. les applications de la technologie SDN
4. Les solutions de la technologie SDN

Flow Routing vs. Aggregation

Les deux modèles sont possibles avec OpenFlow

Model Flow-Based

- Chaque flux est configuré individuellement par le contrôleur
- Entrées de flux ExactOmatch
- Le tableau de flux contient une entrée par flux
- Bon pour le grain fin contrôle, par ex. réseaux de campus

VS

Model Aggregated

- Une entrée de flux couvre de grands groupes de flux
- Entrées de flux génériques
- Le tableau des flux contient une entrée par catégorie de flux
- Bon pour un grand nombre de flux, par ex. colonne vertébrale

Reactive vs. Proactive

Les deux modèles sont possibles avec OpenFlow

Model Reactive

- Premier paquet de contrôleur de déclencheurs de flux à insérer des entrées de flux
- Utilisation efficace du tableau de flux
- Chaque flux nécessite une petite configuration de flux supplémentaire temps
- Si la connexion de contrôle est perdue, le commutateur a une utilité limitée

VS

Model Proactive

- Le contrôleur pré-remplit la table de flux dans le commutateur
- Configuration zéro débit supplémentaire temps
- La perte de contrôle de la connexion ne perturbe pas le trafic
- Nécessite essentiellement agrégé (caractère générique) règles

CHAPITRE 2

Comprendre les Concepts SDN

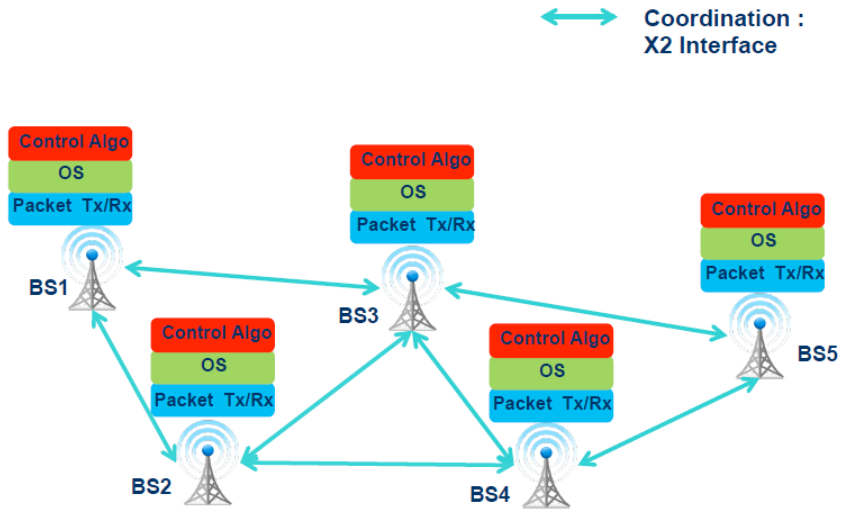
1. Fonctionnement et principe de la technologie SDN
2. Modèles de la technologie SDN
3. Les applications de la technologie SDN
4. Les solutions de la technologie SDN

PARTIE 2

SD-MN -- SOFTRAN

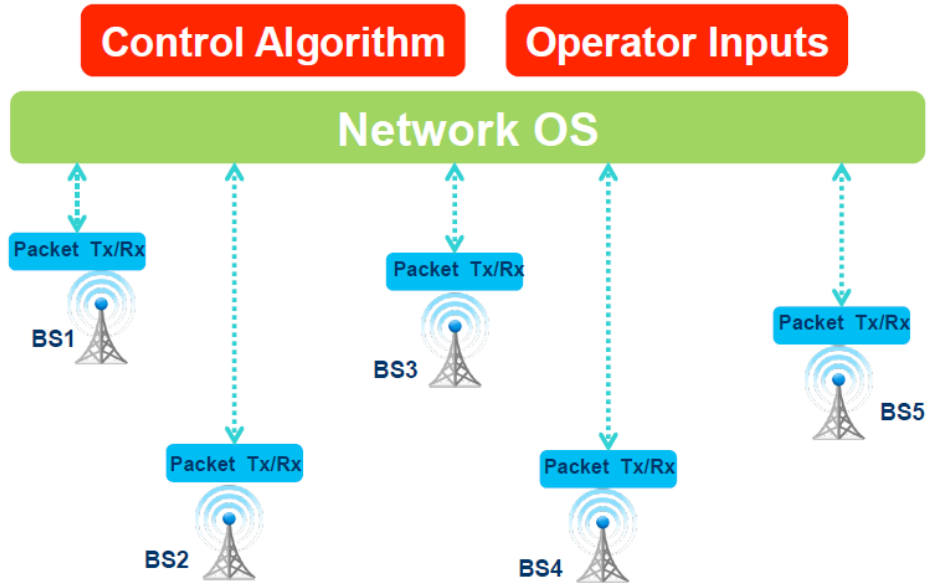
Plan de contrôle distribué

- La signalisation de contrôle augmente avec la densité
- Une coordination étroite devient impossible avec la densité
  - Demandes énormes sur le réseau de liaison
- Gestion inefficace des ressources radio
- Difficile à gérer dans un réseau dense



Plan de contrôle logiquement centralisé :

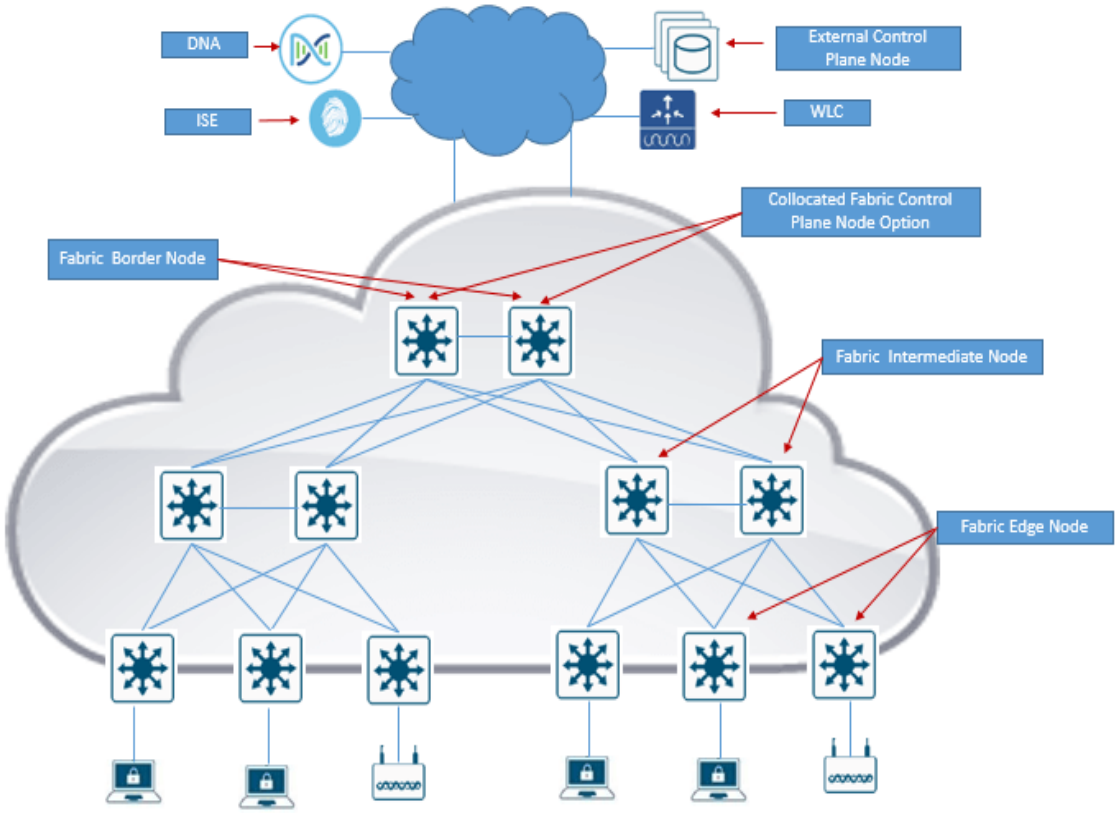
- Vue globale sur les interférences et la charge
  - Coordination facilitée de la gestion des ressources radio
  - Utilisation efficace des ressources sans fil
- Algorithmes de contrôle plug-and-play
  - Gestion simplifiée du réseau
- Des transferts plus fluides
  - Meilleure expérience utilisateur



PARTIE 2

SD-Acces

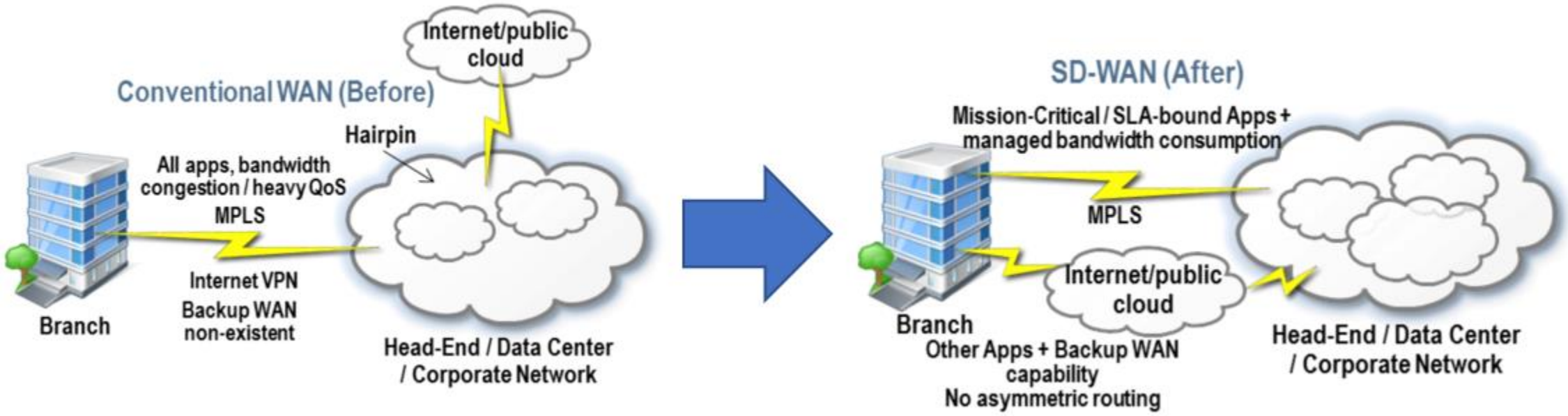
- **Le SD-Access** (SDA : **S**oftware-**D**efined **A**ccess) est une solution **innovante** qui offre une **infrastructure réseau entièrement automatisée et programmable**, permettant ainsi de faire de **grande économie.**
- Le principe repose sur **|** une **« fabric » programmable,** bâtie sur l'ensemble des équipements du réseau de l'entreprise.
- Il utilise une structure réseau unique sur LAN et WLAN pour créer une expérience utilisateur cohérente et hautement sécurisée.
- Il segmente le trafic des utilisateurs, des périphériques et des applications et automatise les politiques d'accès des utilisateurs pour établir la bonne politique pour tout utilisateur ou appareil, avec n'importe quelle application, sur un réseau.
- Permet l'accès au réseau en quelques minutes pour tout utilisateur ou appareil à n'importe quelle application sans compromettre la sécurité.



PARTIE 2

Le SD-WAN selon l'ONUG

- L'ONUG – Open Networking User Group
  - Communauté d'utilisateurs
  - Définition des besoins des grandes entreprises
  - Travaux importants sur le SD-WAN



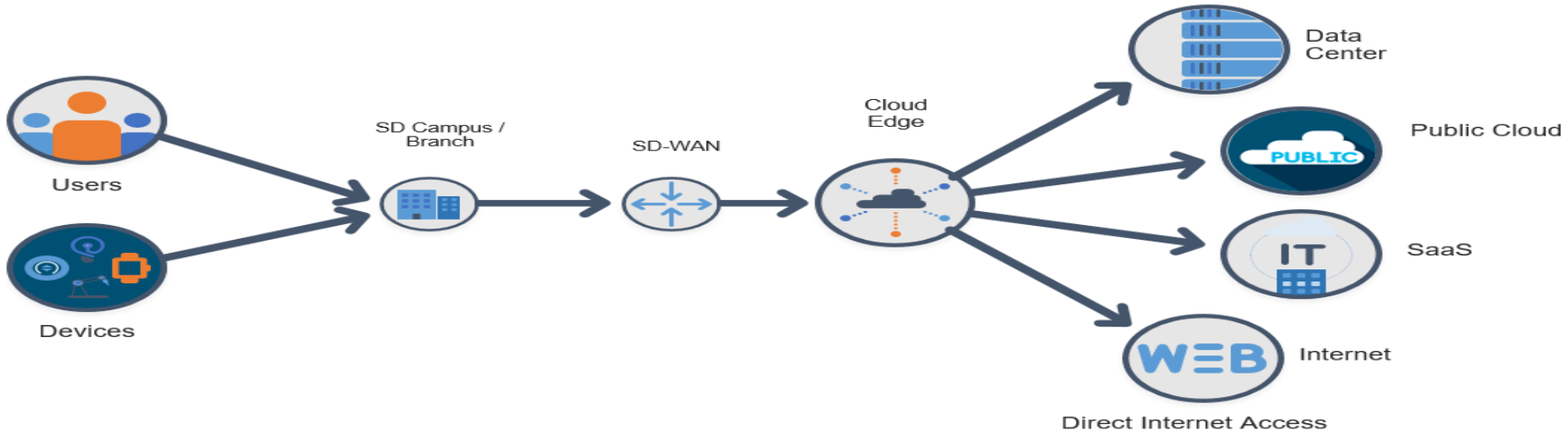
PARTIE 2

La technologie SD-WAN

Le SD-WAN constitue une approche automatisée et programmatique de la gestion de la connectivité et des coûts de circuit des réseaux d'entreprise. Il étend le SDN en le transformant en application que les entreprises peuvent utiliser pour créer rapidement un WAN hybride intelligent.

Les entreprises adoptent rapidement la technologie SD-WAN en raison de ses nombreux avantages financiers et opérationnels:

- Réduit les coûts CapEx et OpEx WAN, ainsi que le coût total de possession.
- Offre la réactivité nécessaire à l'entreprise afin de suivre le rythme des innovations informatiques.
- Prend en charge des connexions multiples, sécurisées et hautes performances, éliminant les pénalités d'accès imposées par les réseaux MPLS.
- Améliore les performances en permettant le partage de la charge entre les connexions et en ajustant les flux de trafic en fonction des conditions du réseau.
- Prend en charge le provisionnement automatisé et les changements apportés aux services réseau haut de gamme tels que les VPN, les pare-feu, la sécurité, l'optimisation WAN et le contrôle de livraison d'applications.
- Prend en charge le provisionnement sans intervention (ZTP).
- Améliore la sécurité du réseau en chiffrant le trafic WAN et en segmentant le réseau afin de minimiser les dommages en cas de violations.



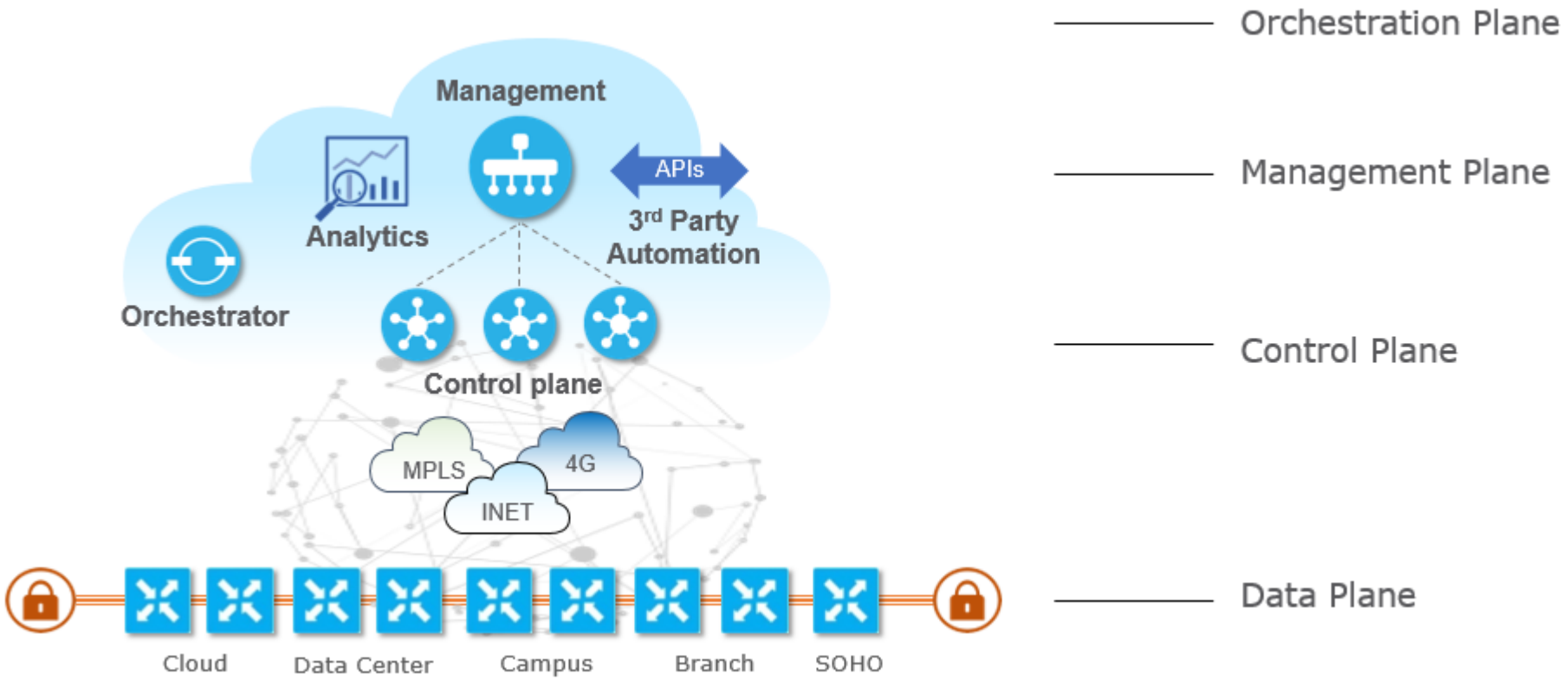
Les pré-requis SD-WAN selon l'ONUG

1. Gestion de plusieurs liens actifs (publics et privés)
2. WAN construit sur des équipements physiques et virtuels
3. WAN hybride sécurisé permettant d'appliquer une ingénierie de trafic par application, prenant en compte la performance des liens
4. Visibilité et priorisation des applications critiques et temps réel selon les règles définies
5. Architecture hautement redondante
6. Intéropérabilité au niveau 2 et 3 avec le reste de l'infrastructure
7. Interface de management centralisée avec tableaux de bord par application, site et VPN
8. Programmabilité de l'infrastructure à travers des API sur un contrôleur qui fournit une abstraction de l'ensemble. Envoi des logs vers collecteurs tiers (SIEM...)
9. Un équipement doit pouvoir être déployé sans configuration et un minimum d'effort sur l'infrastructure actuelle
10. Certification FIPS-140-2 pour le chiffrement

PARTIE 2

Architecture SD-WAN

- n

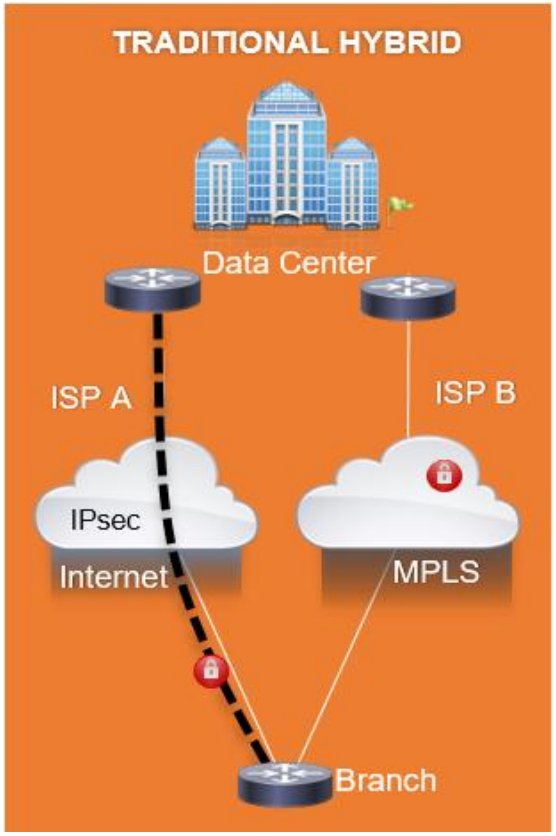


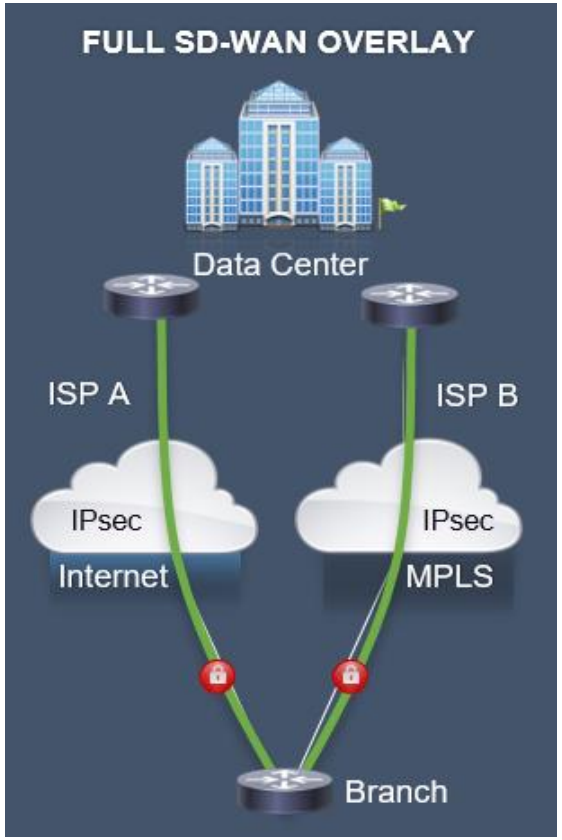
PARTIE 2

WAN hybride et overlay

Le SD-WAN répond aux nouvelles problématiques : le coût , la sécurité, le cloud, la migration.

- **Active/Standby WAN Paths**
- **Two WAN Routing Domains**



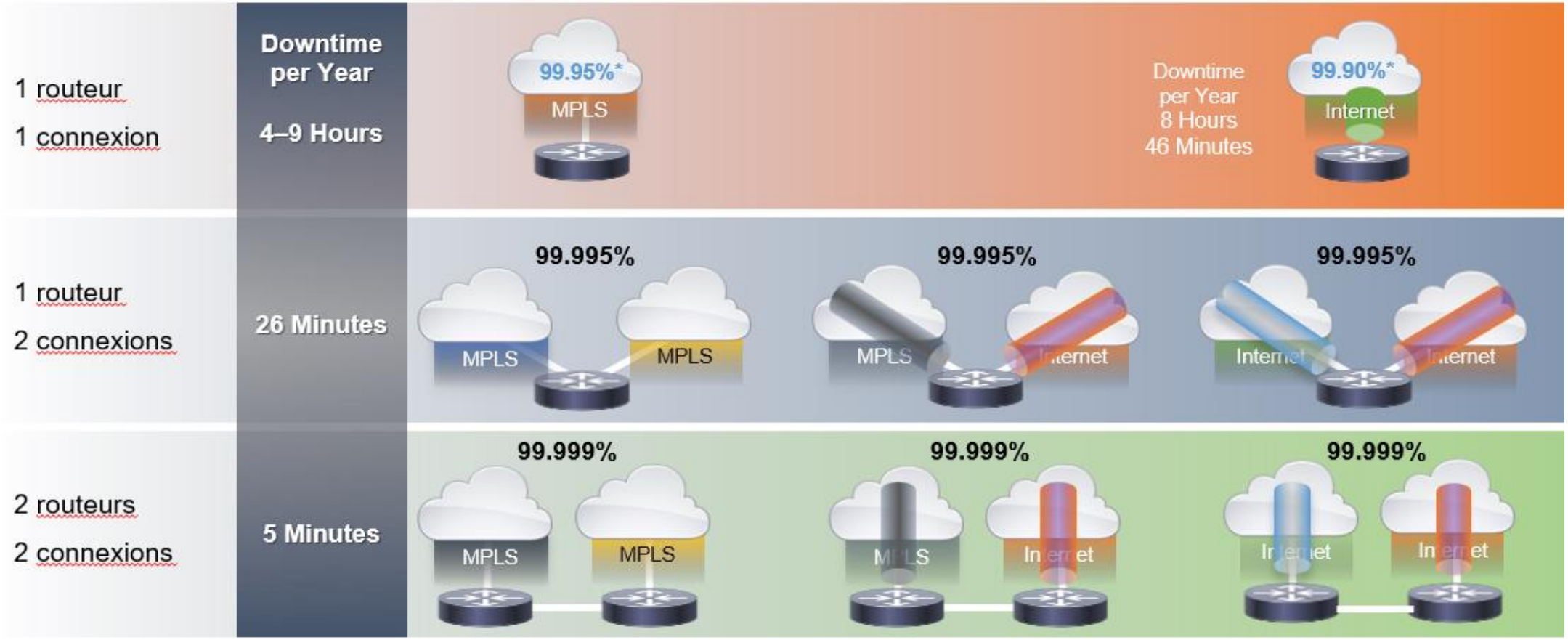


- **Active/Active WAN Paths**
- **One IPsec Overlay**
- **One WAN Routing Domain**

PARTIE 2

La disponibilité du réseau

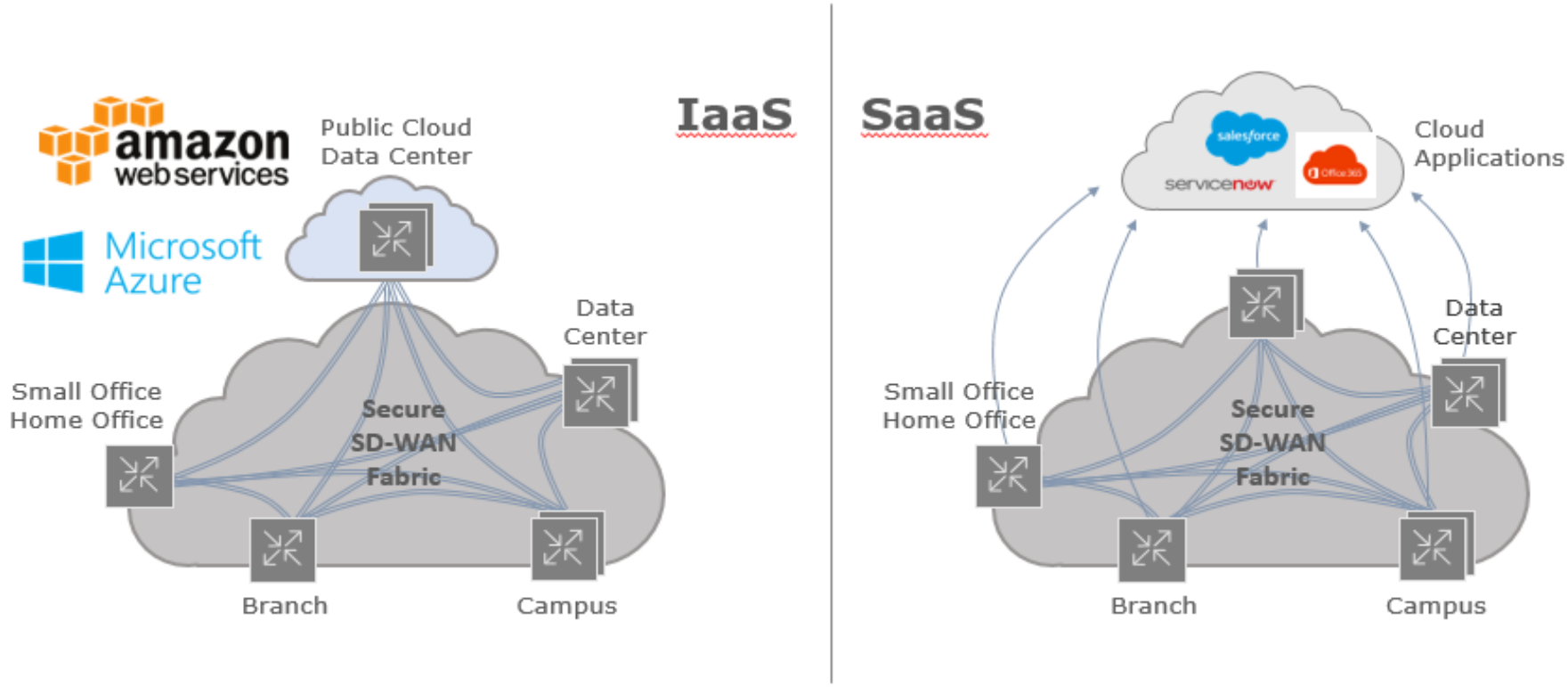
La redondance et la diversité des chemins sont des facteurs plus importants dans la construction de réseaux WAN hautement disponibles.



PARTIE 2

SDWAN avec le cloud

La redondance et la diversité des chemins sont des facteurs plus importants dans la construction de réseaux WAN hautement disponibles.



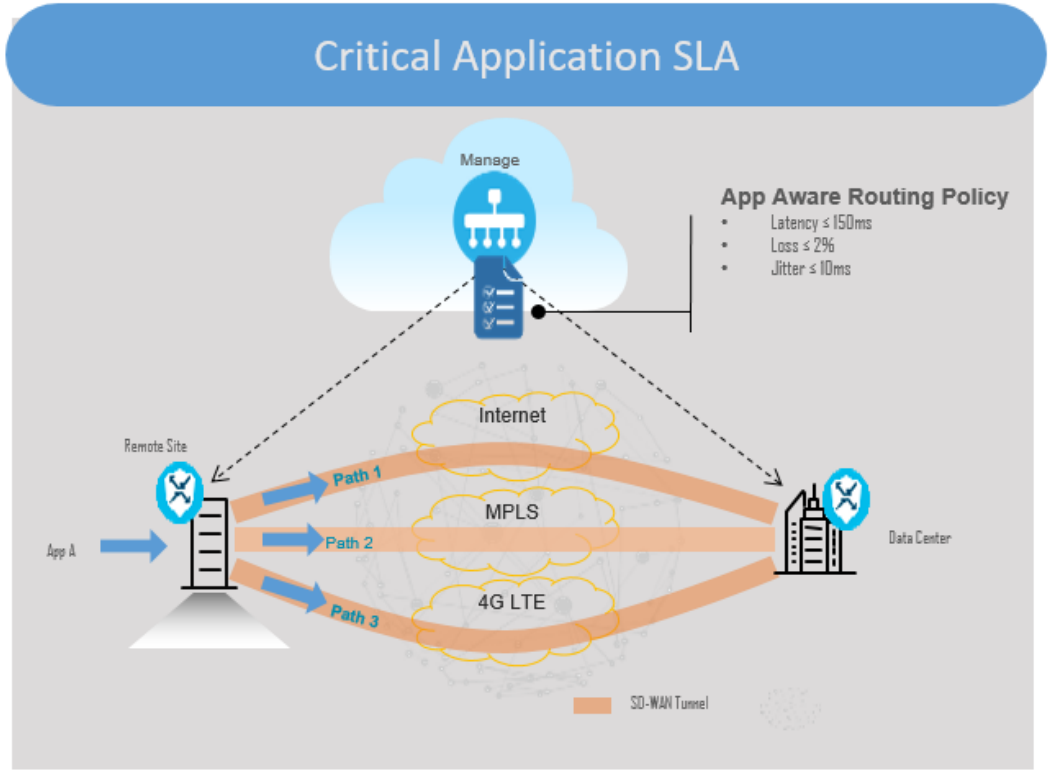
Cloud On-Ramp IaaS

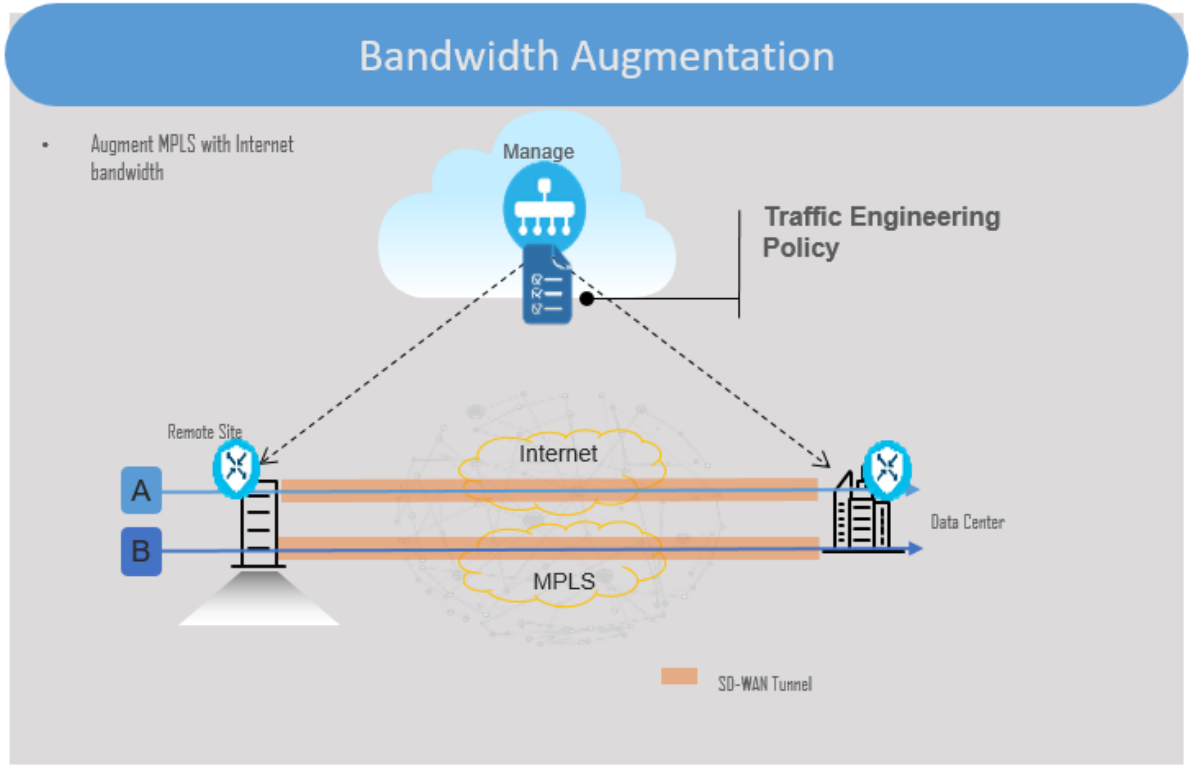
Cloud On-Ramp SaaS

PARTIE 2

Connectivité flexible

Routage sensible aux applications avec n'importe quelle topologie

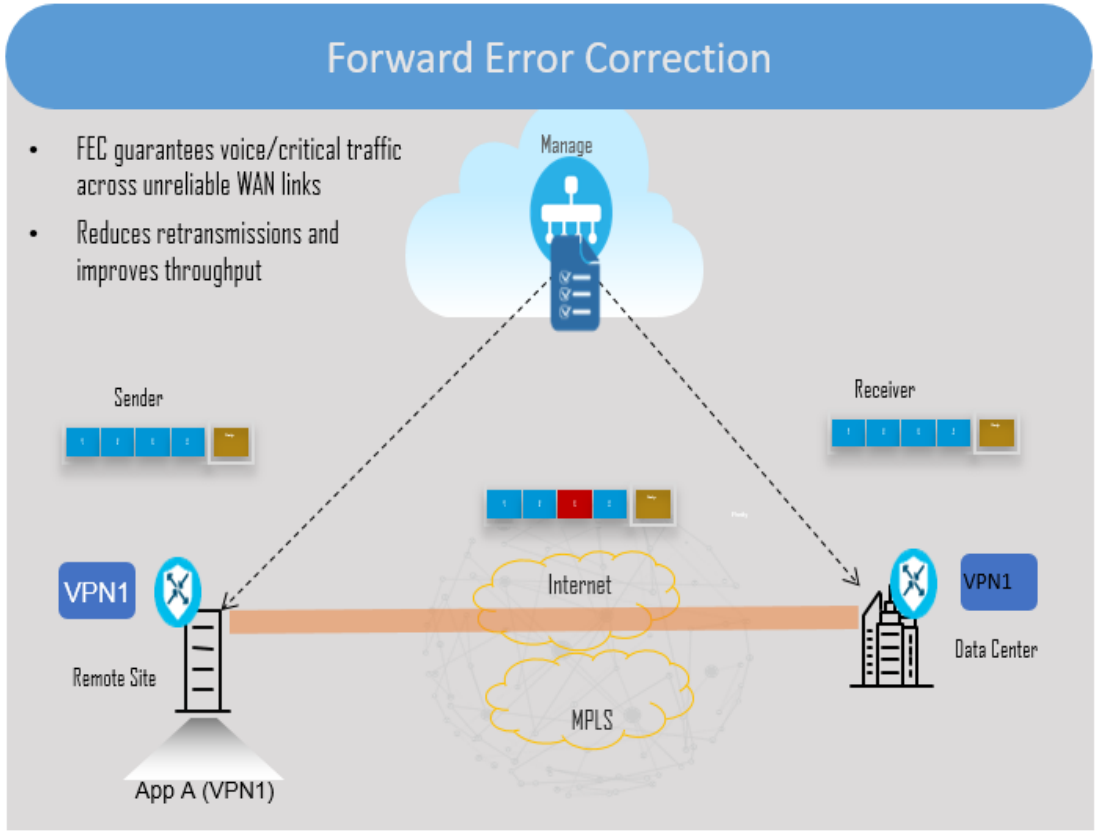


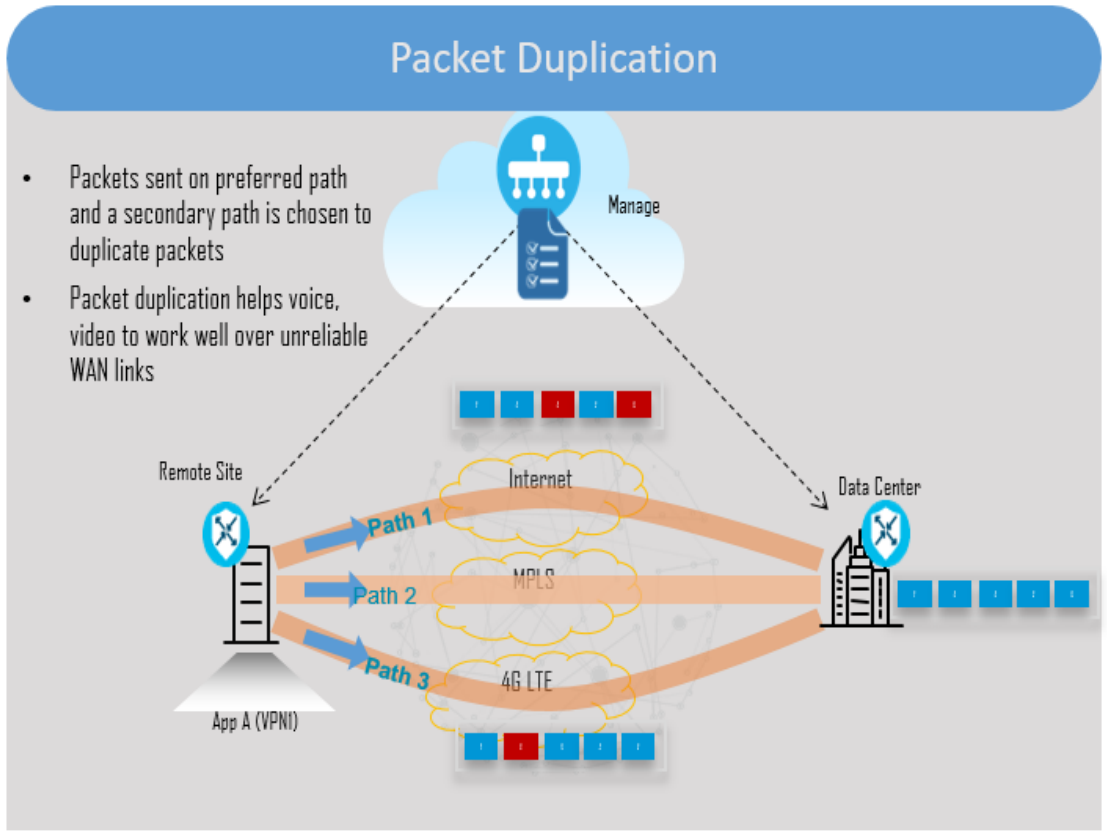


PARTIE 2

Optimisation du trafic voix

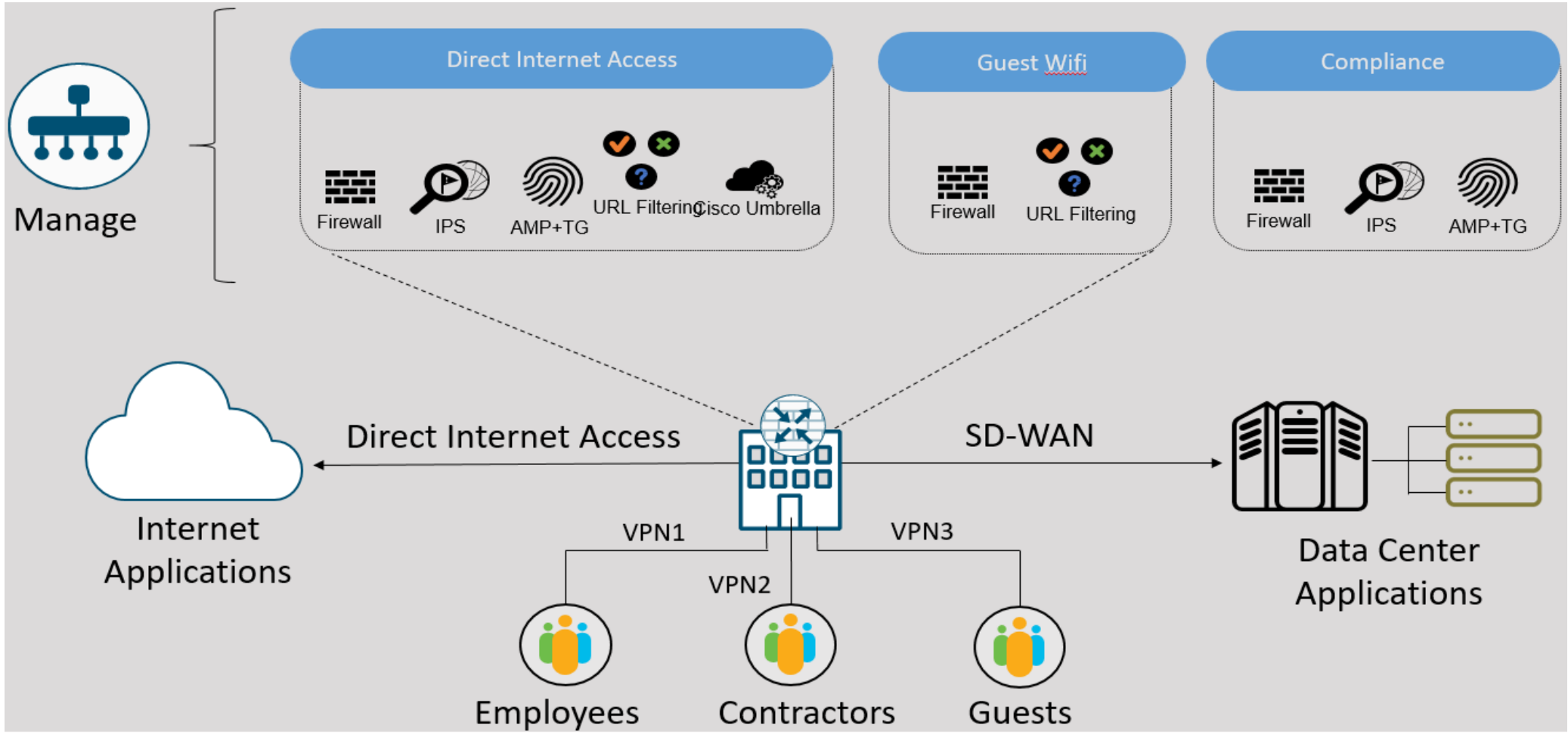
Améliorer la fiabilité avec FEC et la duplication de paquets





PARTIE 2

SD-WAN sécurisé



CHAPITRE 2

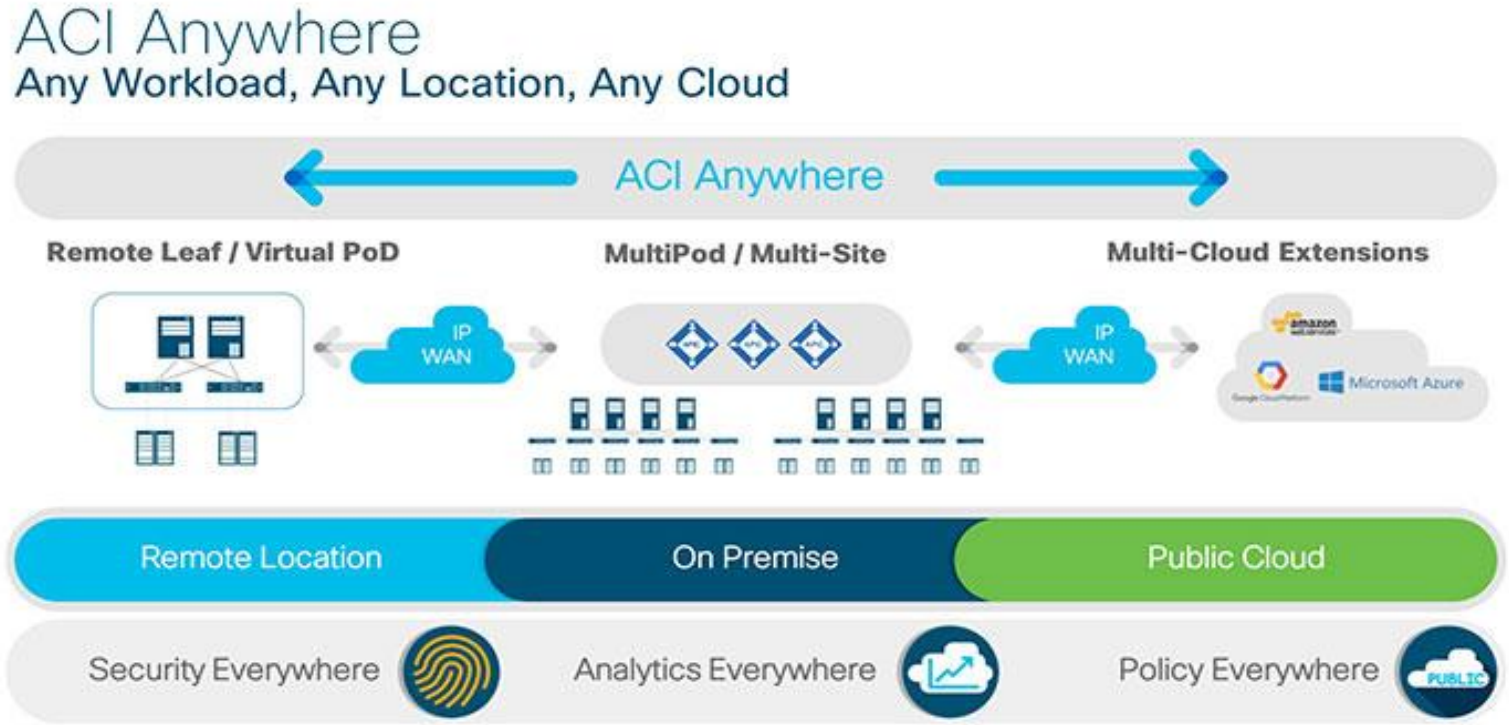
Comprendre les Concepts SDN

1. Fonctionnement et principe de la technologie SDN
2. Modèles de la technologie SDN
3. Les applications de la technologie SDN
4. Les solutions de la technologie SDN

PARTIE 2

Cisco ACI (Application Centric Infrastructure)

- Une solution matérielle spécialement conçue pour intégrer le cloud computing et la gestion des centres de données.
- Cisco ACI est une solution SDN de pointe qui offre une automatisation basée sur des politiques par le biais d'une surcouche et d'une sous-couche intégrées. Elle est indépendante de l'hyperviseur et étend l'automatisation des politiques à tous les workloads, y compris les machines virtuelles, les serveurs physiques sans système d'exploitation et les containers.

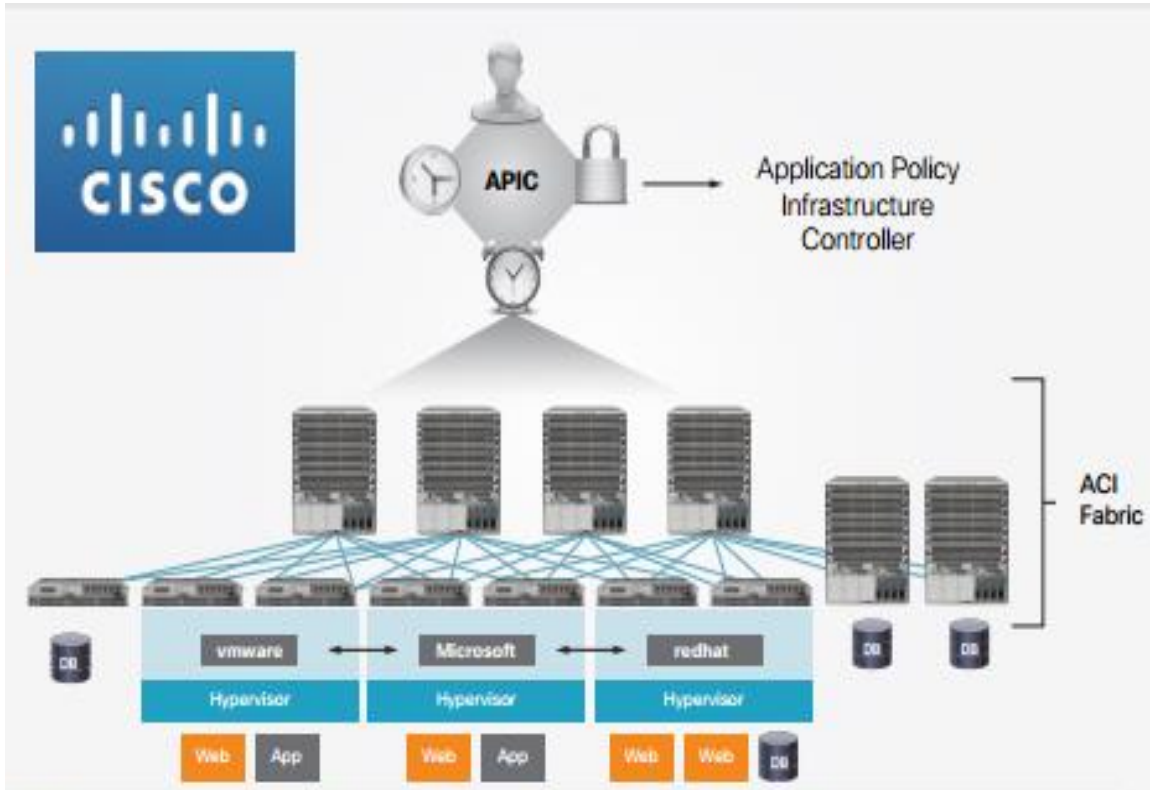


Cisco ACI (Application Centric Infrastructure)

Cisco ACI est une solution matérielle spécialisée offrant une gestion intégrée du cloud computing et du data center. Au niveau global, tout élément relatif à la politique du réseau est retiré du plan de données. Cela permet de créer beaucoup plus facilement les réseaux de data center.

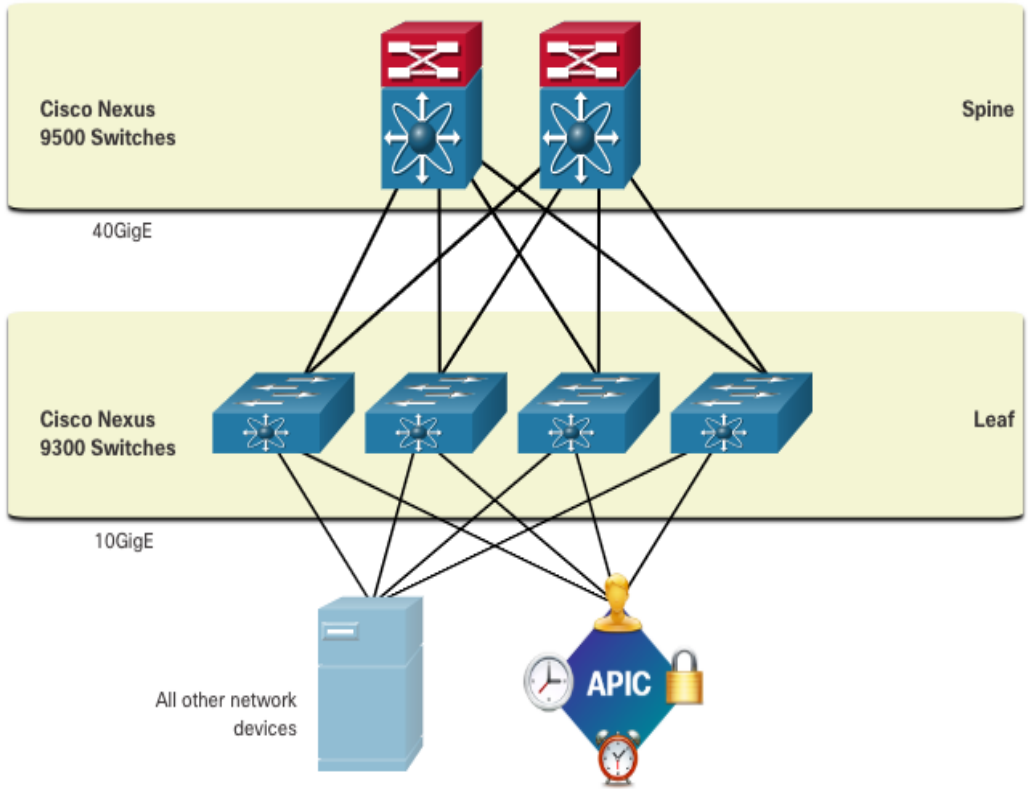
Les trois principaux composants de l'architecture ACI:

- **Profil de réseau d'application (ANP)**
- **Contrôleur de l'infrastructure des règles régissant les applications (APIC)**
- **Commutateurs Cisco Nexus série 9000**



Topologie Spine-Leaf

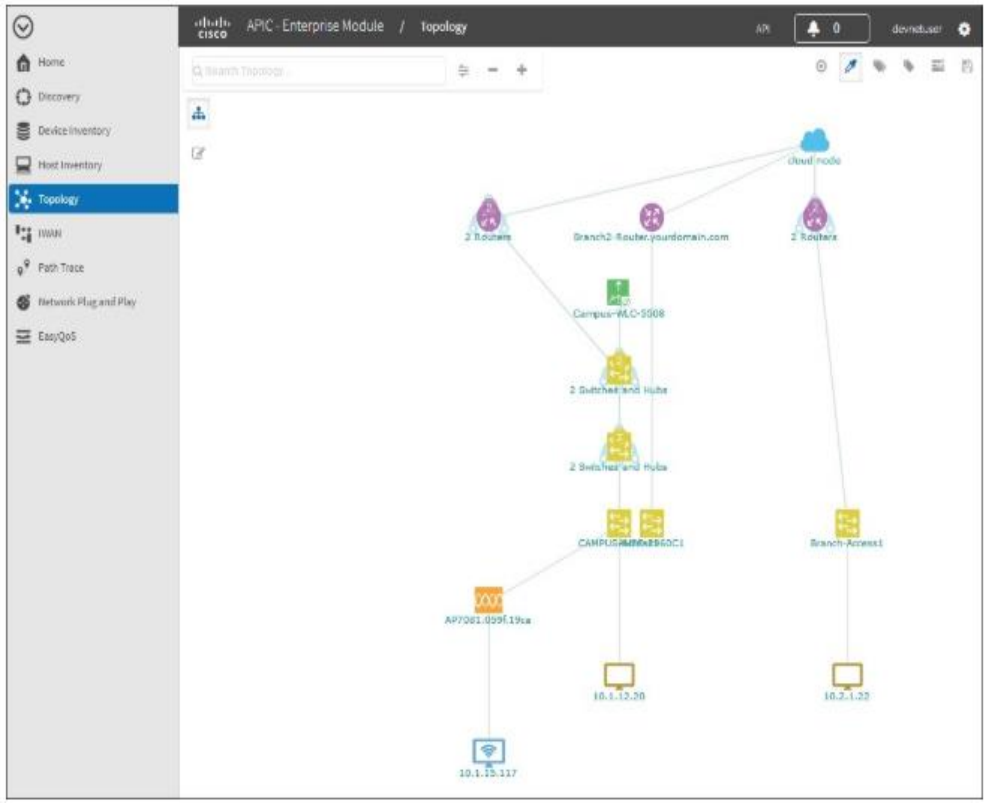
- Comme le montre la figure, le fabric Cisco ACI se compose du contrôleur APIC et des commutateurs Cisco Nexus 9000 dans une topologie Spine-Leaf à deux niveaux.
- Les commutateurs Leaf sont associés à des commutateurs Spine, mais ne le sont jamais entre eux. De même, les commutateurs Spine sont uniquement associés à des commutateurs Leaf et centraux (non représentés). Dans cette topologie à deux niveaux, tous les éléments ne sont qu'à un « saut » les uns des autres.
- Contrairement à ce qui se passe dans une infrastructure SDN, le contrôleur APIC ne manipule pas directement le chemin des données. Au lieu de cela, il centralise la définition des stratégies et programme les commutateurs Leaf de manière à ce qu'ils transfèrent le trafic en fonction des politiques définies.



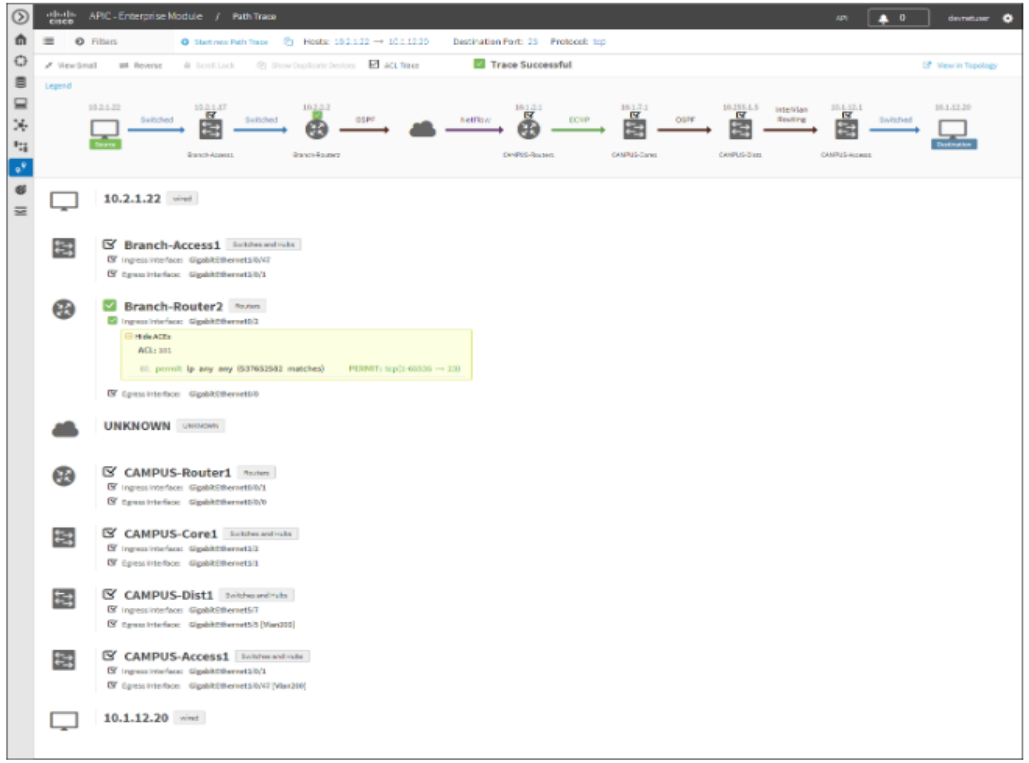
PARTIE 2

Cisco APIC-EM

Cisco APIC-EM fournit une interface unique pour la gestion du réseau.

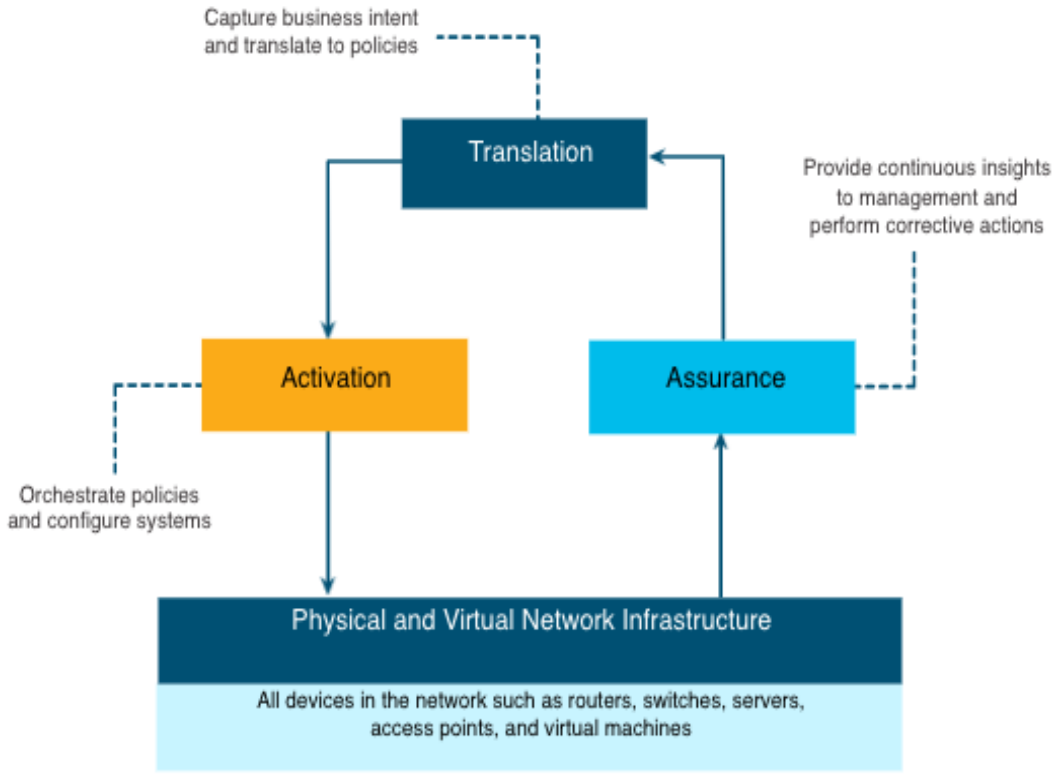


L'outil APIC-EM Path Trace permet à l'administrateur de visualiser facilement les flux de trafic et de découvrir toute entrée de ACL conflictuelle, dupliquée ou occultée.



Présentation de réseau basée sur l'intention

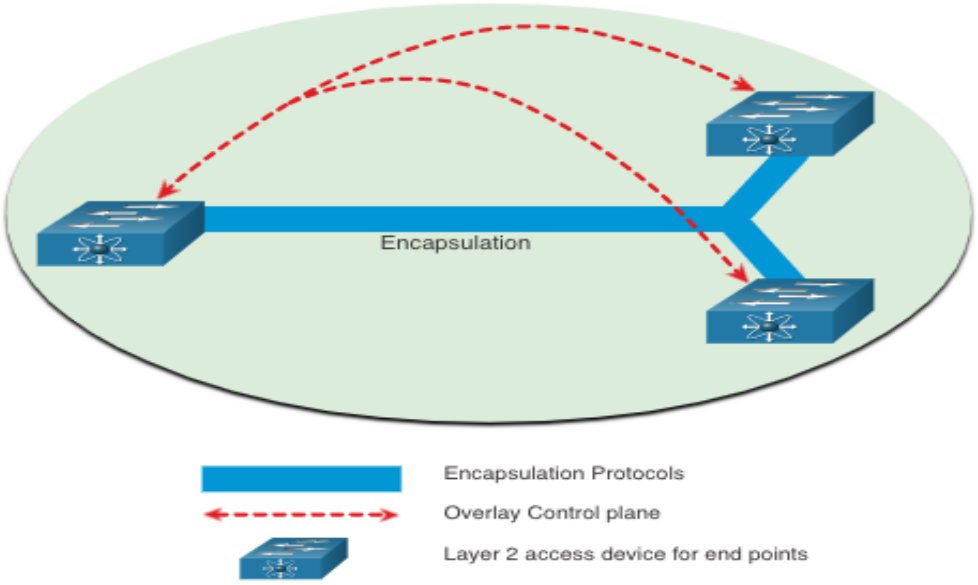
- IBN est le modèle industriel émergent de la prochaine génération de réseaux. IBN s'appuie sur un réseau défini par logiciel (SDN), transformant une approche matérielle et manuelle de la conception et de l'exploitation des réseaux en une approche centrée sur le logiciel et entièrement automatisée.
- Les objectifs commerciaux du réseau sont exprimés comme intention. IBN capture l'intention de l'entreprise et utilise l'analyse, l'apprentissage automatique et l'automatisation pour aligner le réseau de manière continue et dynamique à mesure que les besoins de l'entreprise évoluent.
- IBN capture et traduit l'intention de l'entreprise en politiques de réseau qui peuvent être automatisées et appliquées de manière cohérente à travers le réseau.
- Cisco considère IBN comme ayant trois fonctions essentielles: la traduction, l'activation et l'assurance. Ces fonctions interagissent avec l'infrastructure physique et virtuelle sous-jacente, comme illustré dans la figure.

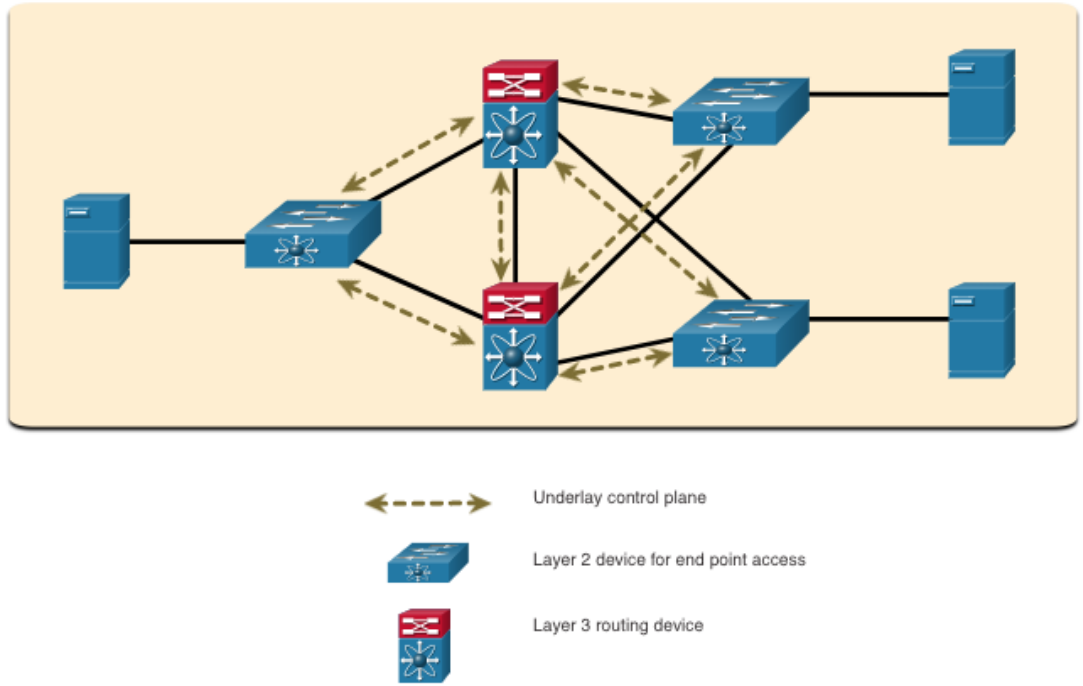


PARTIE 2

Réseau de IBN

Du point de vue d'IBN, l'infrastructure de réseau physique et virtuel est un tissu; une superposition qui représente la topologie logique utilisée pour se connecter virtuellement aux périphériques. Et un réseau sous-jacent qui représente la topologie physique qui comprend tout le matériel requis pour atteindre les objectifs commerciaux.

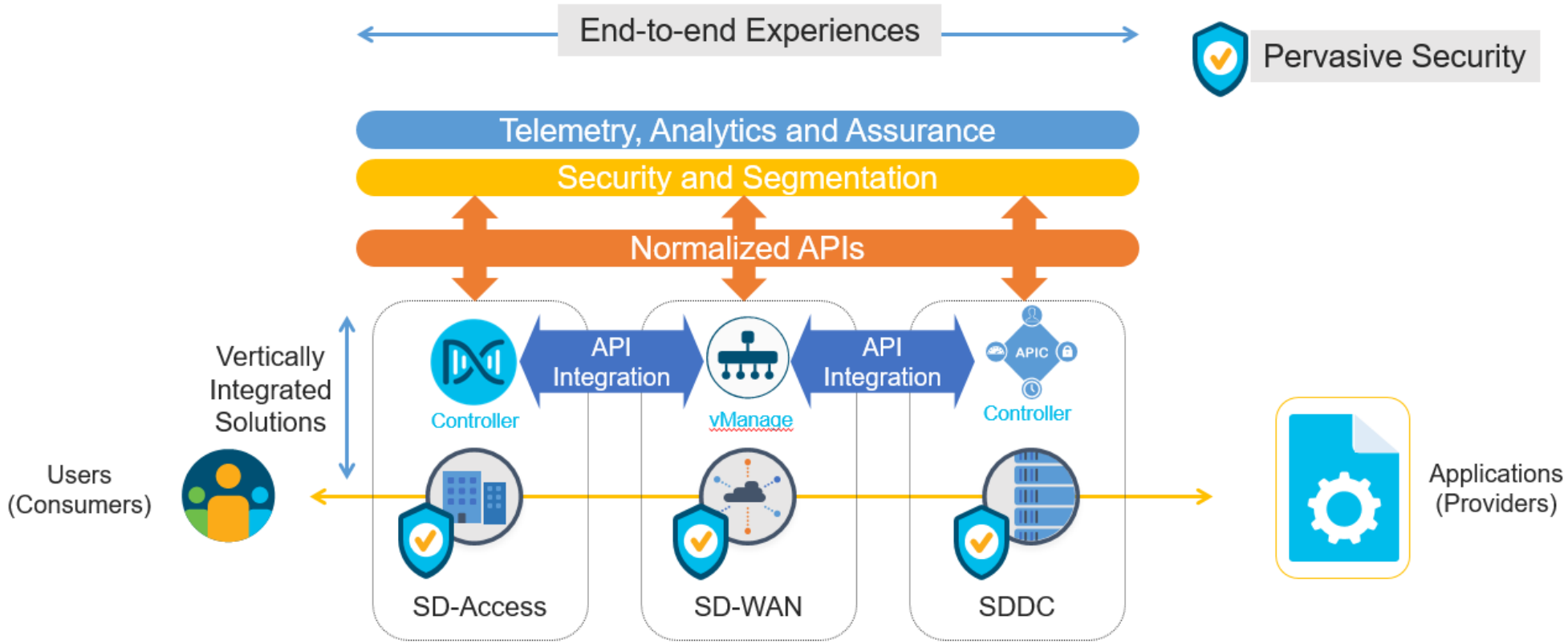




PARTIE 2

Interconnecte les réseaux multi-domaines

- Centre

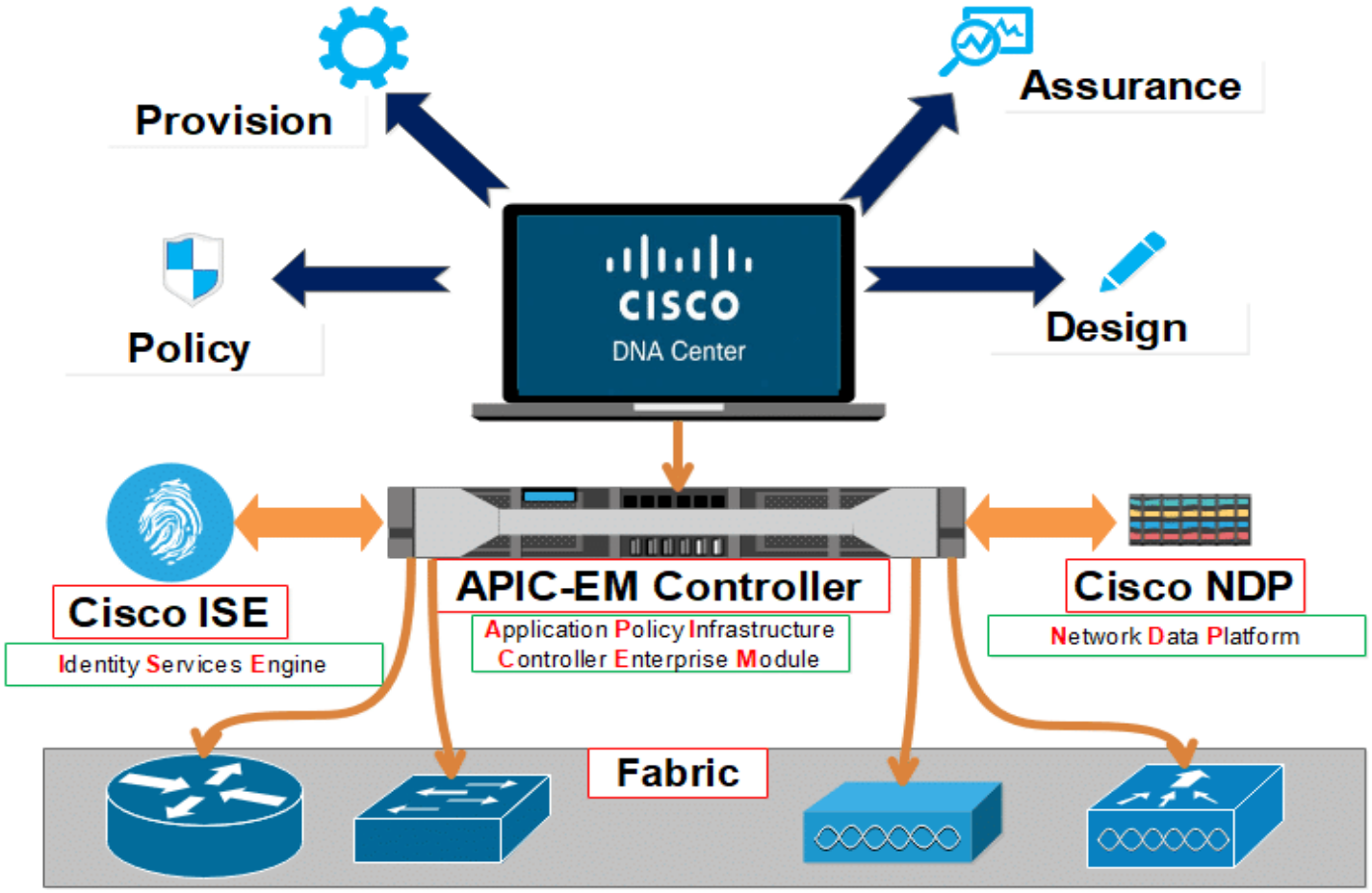


Solution de Cisco DNA

Solution de Cisco DNA	Description	Bénéfices
SD-Access	•Première solution de mise en réseau d'entreprise basée sur l'intention construite avec Cisco DNA. •Il utilise une structure réseau unique sur LAN et WLAN pour créer une expérience utilisateur cohérente et hautement sécurisée. •Il segmente le trafic des utilisateurs, des périphériques et des applications et automatise les politiques d'accès des utilisateurs pour établir la bonne politique pour tout utilisateur ou appareil, avec n'importe quelle application, sur un réseau.	Permet l'accès au réseau en quelques minutes pour tout utilisateur ou appareil à n'importe quelle application sans compromettre la sécurité.
SD-WAN	•Il utilise une architecture cloud sécurisée pour gérer de manière centralisée les connexions WAN. •Il simplifie et accélère la fourniture de services WAN sécurisés, flexibles et riches pour connecter les centres de données, les branches, les campus et les installations de colocation.	•Offre une meilleure expérience d'utilisateur pour les applications résidant sur site ou dans le cloud. •Obtenez une plus grande agilité et des économies de coûts grâce à des déploiements plus faciles et à l'indépendance de transport.
Assurance de Cisco DNA	•Utilisé pour dépanner et augmenter la productivité informatique. •Il applique des analyses avancées et un apprentissage automatique pour améliorer les performances et la résolution des problèmes, et prévoir d'assurer les performances du réseau. •Il fournit une notification en temps réel pour les conditions de réseau qui nécessitent une attention.	•Vous permet d'identifier les causes profondes et propose une correction suggérée pour un dépannage plus rapide. •Le Cisco DNA Center fournit un tableau de bord unique facile à utiliser avec des informations et des capacités d'exploration. •L'apprentissage automatique améliore continuellement l'intelligence du réseau pour prévoir les problèmes avant qu'ils ne surviennent.
Sécurité Cisco DNA	•Utilisé pour fournir une visibilité en utilisant le réseau comme capteur pour l'analyse et l'intelligence en temps réel. •Il offre un contrôle granulaire augmenté pour appliquer la politique et contenir les menaces sur le réseau.	•Réduire les risques et protéger votre organisation contre les menaces, même dans le trafic chiffré. •Obtenir une visibilité à 360 degrés grâce à des analyses en temps réel pour une intelligence profonde à travers le réseau. •Diminuer la complexité avec une sécurité de bout en bout.

PARTIE 2

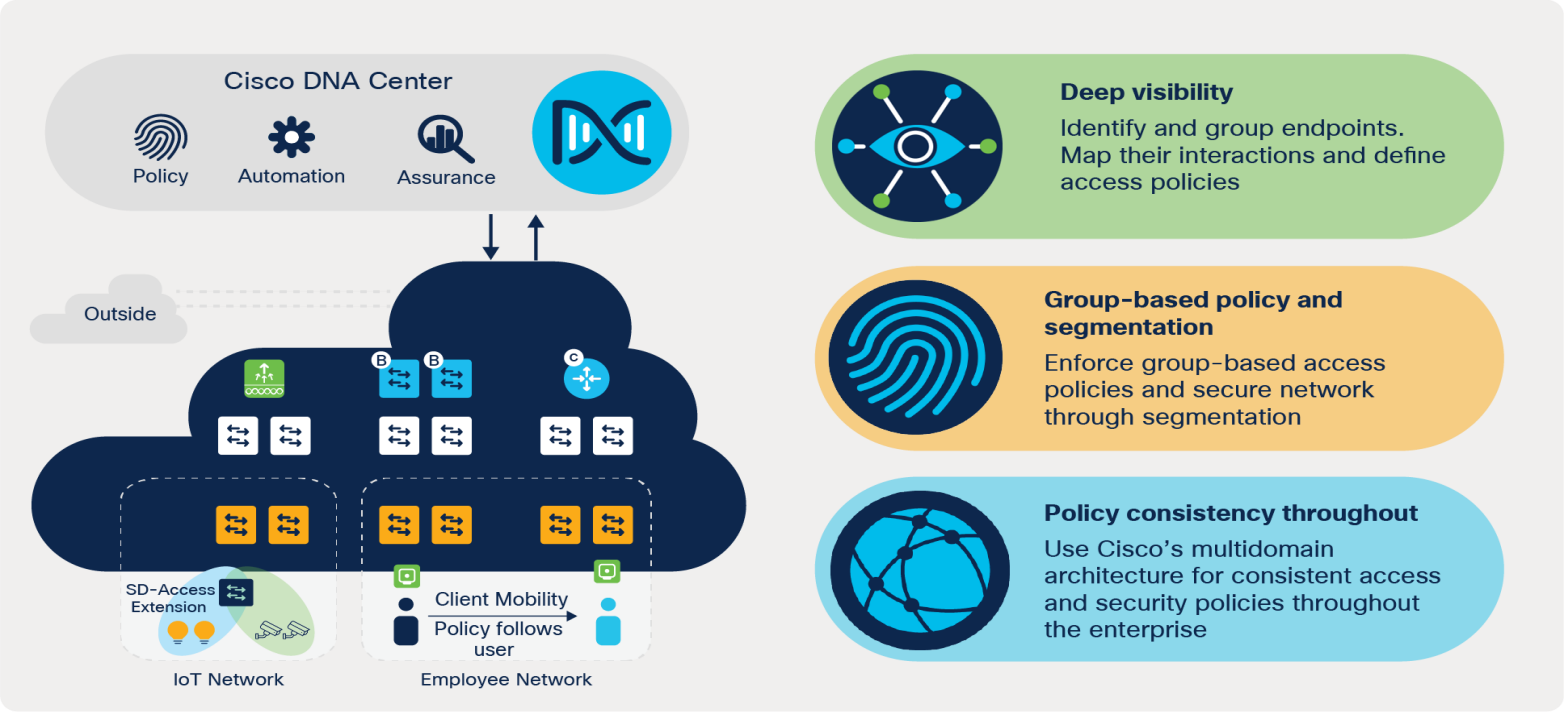
Solution de Cisco DNA



PARTIE 2

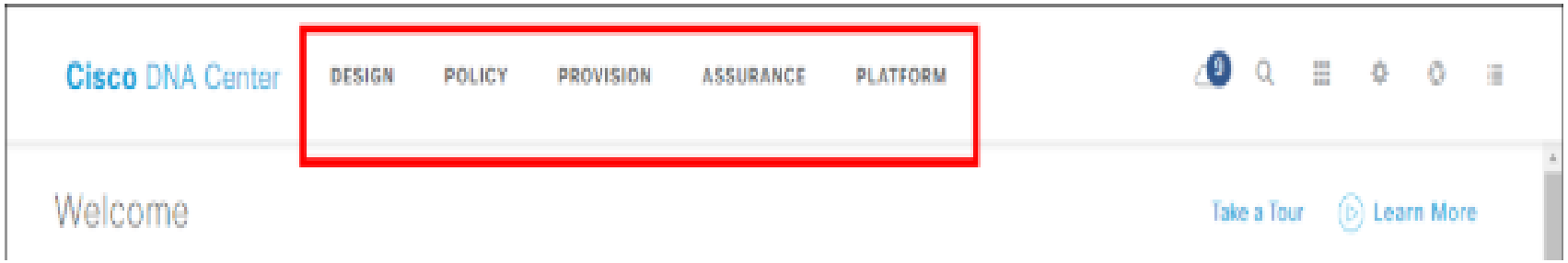
Centre de Cisco DNA

- Centre de Cisco DNA correspond au contrôleur de base et à la plate-forme d'analytique au cœur de Cisco DNA. Il prend en charge l'expression d'intention pour plusieurs cas d'utilisation, y compris les capacités d'automatisation de base, le provisionnement de tissu et la segmentation basée sur des politiques dans le réseau d'entreprise.
- Cisco DNA Center est un centre de gestion et de commande de réseau pour l'approvisionnement et la configuration des périphériques de réseau. Il s'agit d'une plate-forme matérielle et logicielle fournissant une «vitre unique» (interface unique) axée sur l'assurance, l'analytique et l'automatisation.



Interface du plate-forme DNA

- La page de lancement de l'interface du centre de DNA vous donne un résumé général de la santé et un instantané du réseau. À partir de là, l'administrateur de réseau peut rapidement explorer les domaines d'intérêt.



En haut, les menus vous permettent d'accéder aux cinq zones principales du centre de DNA. Comme indiqué dans la figure, ce sont:

- **Conception** - Modélisez votre réseau, des sites et bâtiments aux périphériques et liaisons, physiques et virtuels, sur le campus, la branche, le WAN et le cloud.
- **Politique** - Utilisez des politiques pour automatiser et simplifier la gestion du réseau, en réduisant les coûts et les risques tout en accélérant le déploiement de services nouveaux et améliorés.
- **Provision** - Fournissez de nouveaux services aux utilisateurs avec facilité, rapidité et sécurité sur votre réseau d'entreprise, indépendamment de la taille et de la complexité du réseau.
- **Assurance** - Utilisez une surveillance proactive et des informations provenant du réseau, des périphériques et des applications pour prévoir les problèmes plus rapidement et garantir que les changements de politique et de configuration atteignent l'objectif commercial et l'expérience de l'utilisateur que vous souhaitez.
- **Platform** - Utilisez les API pour vous intégrer à vos systèmes informatiques préférés pour créer des solutions de bout en bout et ajouter la prise en charge des périphériques multifournisseurs.

CHAPITRE 3

Etudier le protocole et les contrôleurs OpenFlow

Ce que vous allez apprendre dans ce chapitre :

- Architecture du protocole OpenFlow

8 heures

CHAPITRE 3

Etudier le protocole et les contrôleurs OpenFlow

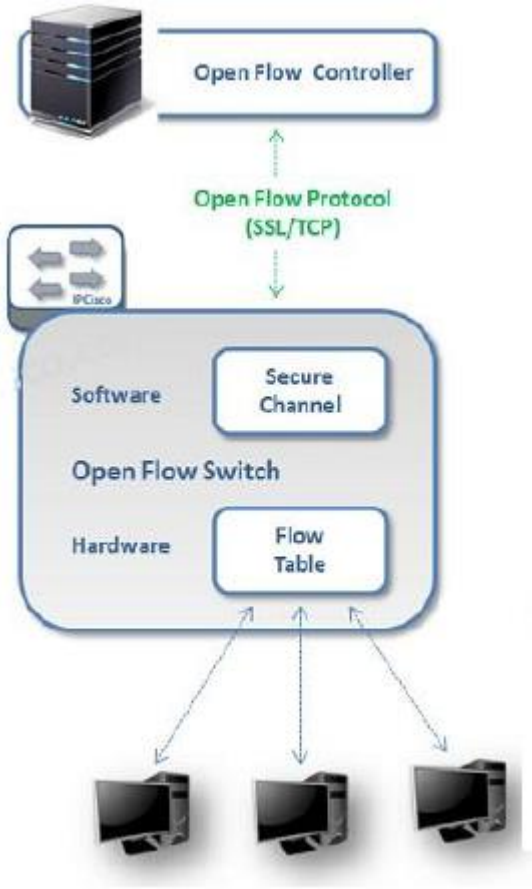
1. Architecture du protocole OpenFlow
2. Flow Table et Les messages Openflow
3. OpenFlow Switches

03 -Etudier le protocole et les contrôleurs OpenFlow

Présentation du protocole OpenFlow

Le protocole OpenFlow

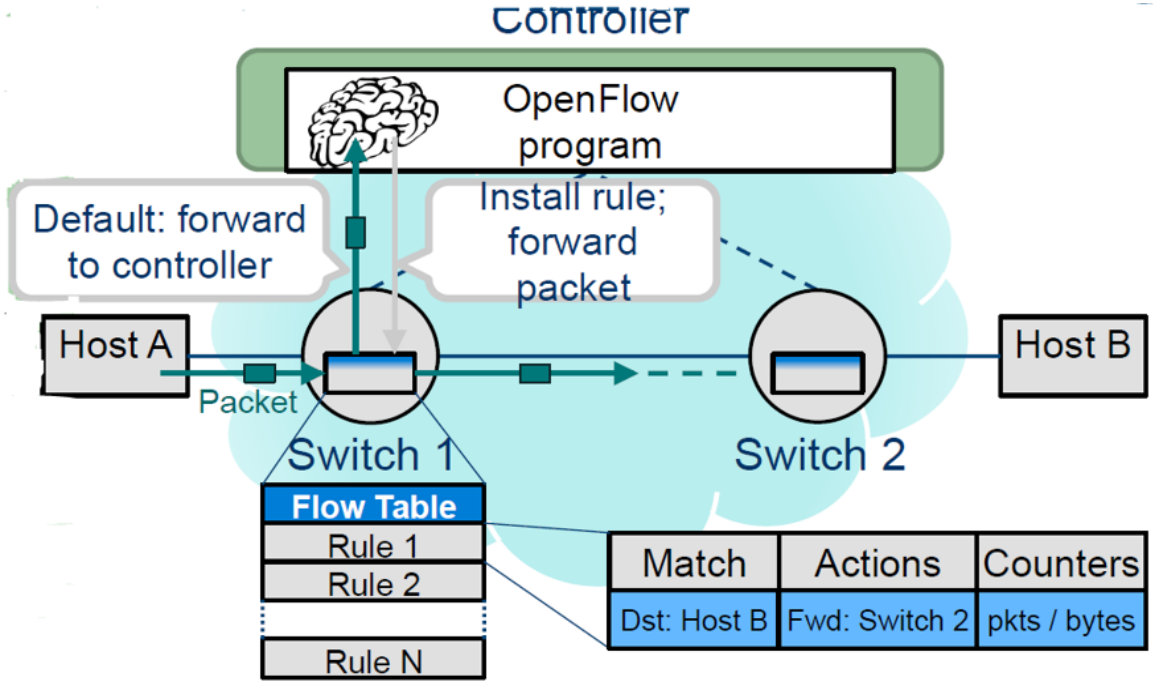
- OpenFlow est un protocole pour contrôler à distance la table de transfert d'un commutateur ou d'un routeur. Est un élément important du SDN
- OpenFlow est similaire à un jeu d'instructions x86 pour le réseau Fournir une interface ouverte au nœud de réseau « boîte noire »
- Cette approche a été développée à l'université de Stanford pour gérer le trafic entre les routeurs, les commutateurs, les points d'accès sans fil et un contrôleur.

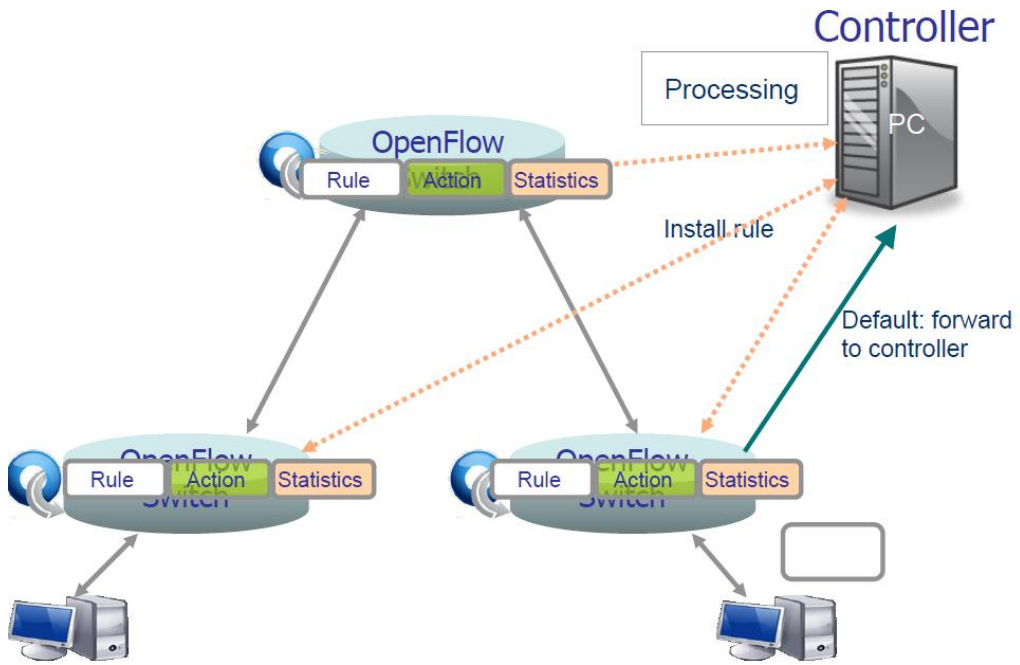


PARTIE 2

PARTIE 2

Architecture du protocole OpenFlow





PARTIE 2

Les version du protocole OpenFlow

Evolution of the specification: Mature and Evolve

"Working code before new standards"

"ONF should not anoint a single reference implementation but instead encourage open-source implementations"; ONF board encourages multiple reference implementations

OpenFlow 1.0.X : no work planned

OpenFlow 1.3.X: long term support

OpenFlow 1.4: extensibility, incremental improvements

CHAPITRE 3

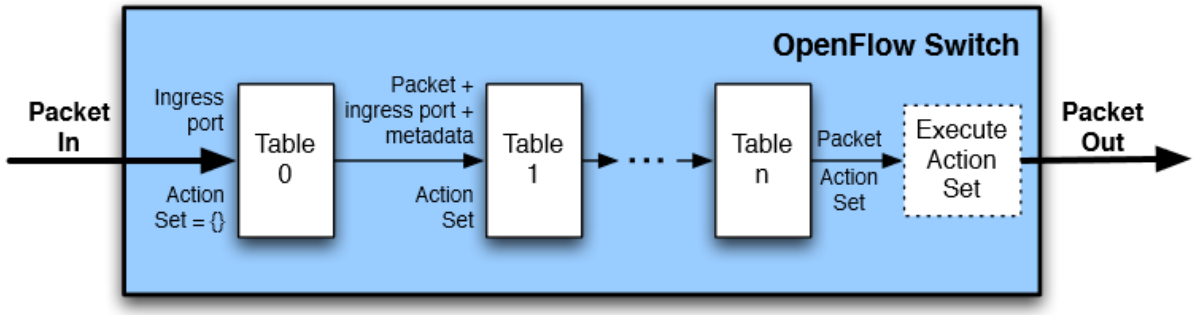
Etudier le protocole OpenFlow

1. Architecture du protocole OpenFlow
2. Flow Table et Les messages Openflow
3. OpenFlow Switches
4. Architecture et le fonctionnement du contrôleur

Flow entry

Le Pipeline OpenFlow

- C'est une succession de plusieurs tables de flux par rapport auxquelles les paquets sont analysés (les
- tables sont numérotées à partir de 0, le nombre maximal n'est limité que par **OFPTT_MAX**)



(a) Packets are matched against multiple tables in the pipeline

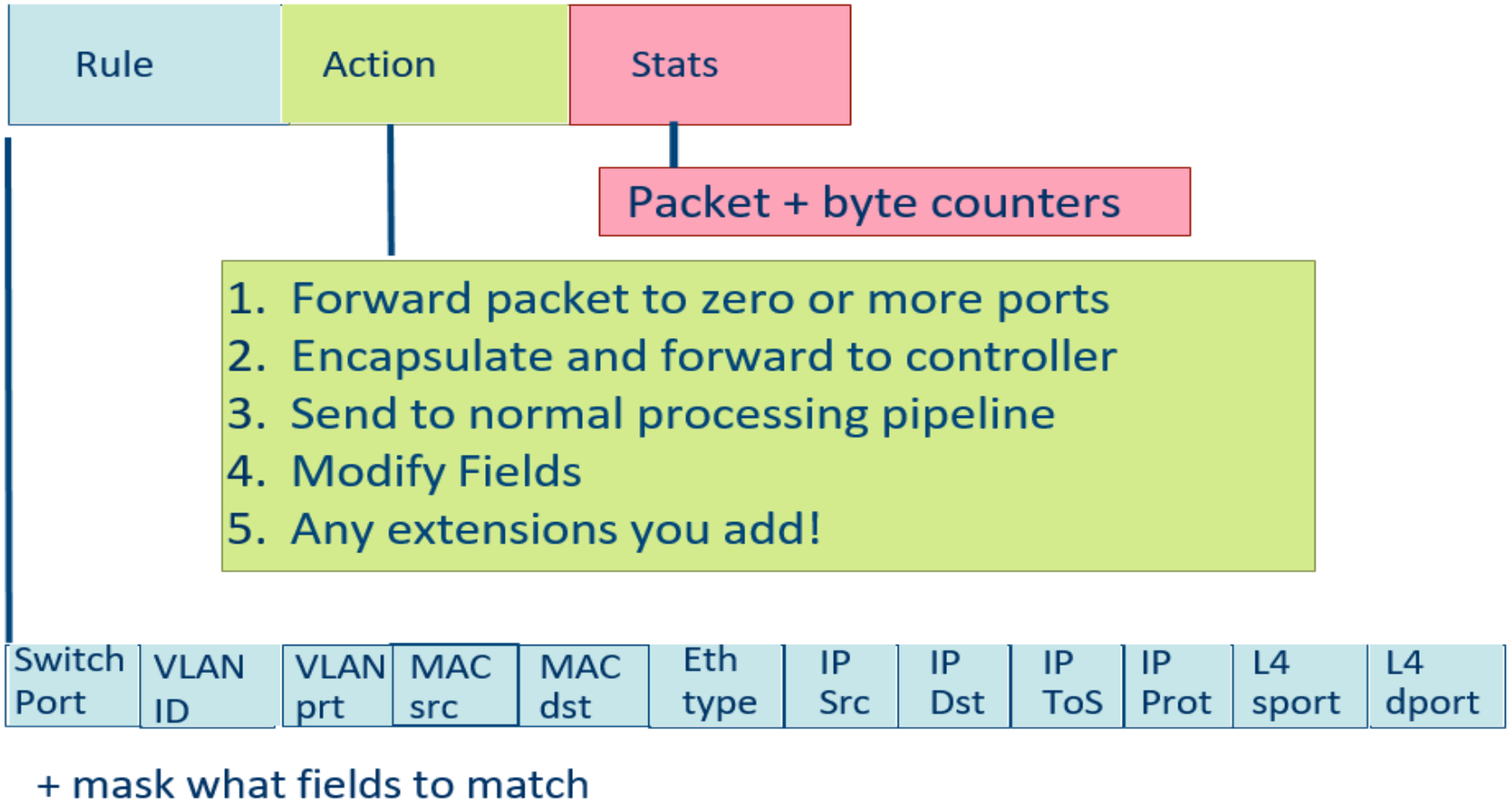
- Les critères de traitement des paquets au sein d'une table de flux sont:
  - Le port d'entrée
  - Les en-têtes du paquet (tous les champs)
  - Optionnellement : Métadonnées spécifiées par la table précédente (les métadonnées sont utilisées pour passer des informations entre les tables : modifications opérées sur les entêtes du paquet par exemple)

PARTIE 2

PARTIE 2

Flow table

- Le

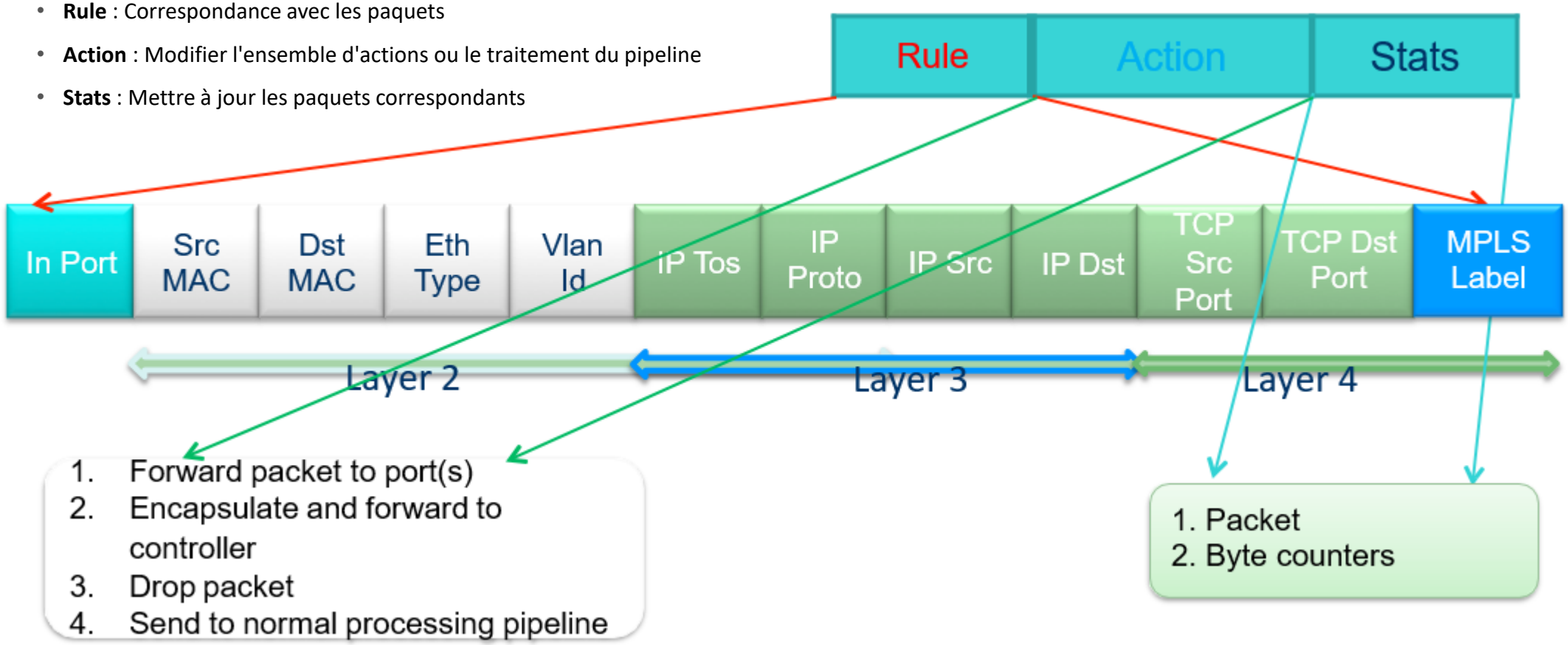


PARTIE 2

Flow entry

Une entrée de flux consiste en

- **Rule** : Correspondance avec les paquets
- **Action** : Modifier l'ensemble d'actions ou le traitement du pipeline
- **Stats** : Mettre à jour les paquets correspondants



OpenFlow Messages

- Table de flux (Flow table)

Match Fields	Priority	Counters	Instructions	Timeouts	Cookie

Table 1: Main components of a flow entry in a flow table.

- Match Field (**ID**) : champ défini comme critère de comparaison du paquet
  - Ingress port
  - en-têtes (L2/L3/L4)
  - Métadonnées (optionnelle)
- Priority (**ID**): pour prioriser les entrées de la table de flux
- Counters : à mettre à jour en cas de correspondance
- Instructions: pour modifier l'ensemble des actions ou le traitement pipeline
- Timeouts : le temps maximum avant qu'un flux n'expire
- Cookie : données utilisées par le contrôleur pour filtrer les statistiques de flux par type

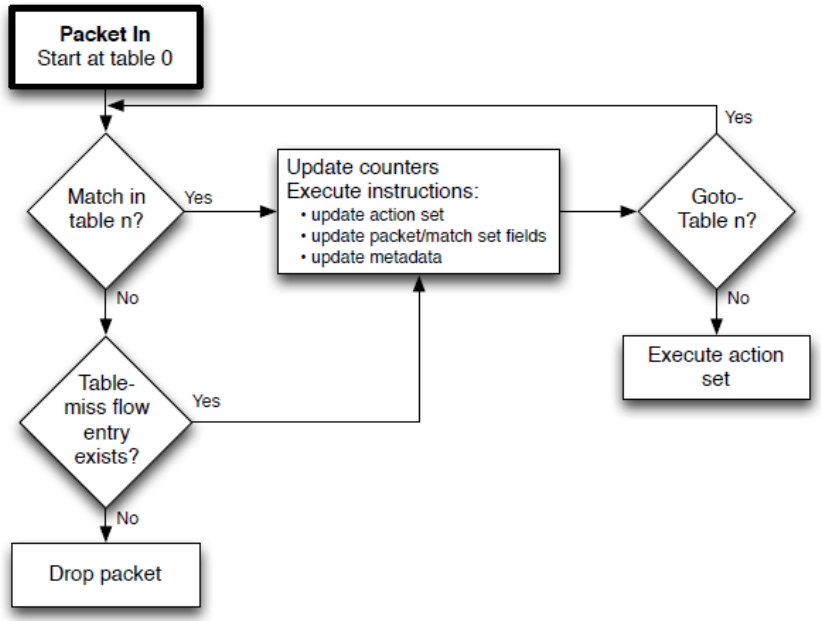


Figure 3: Flowchart detailing packet flow through an OpenFlow switch.

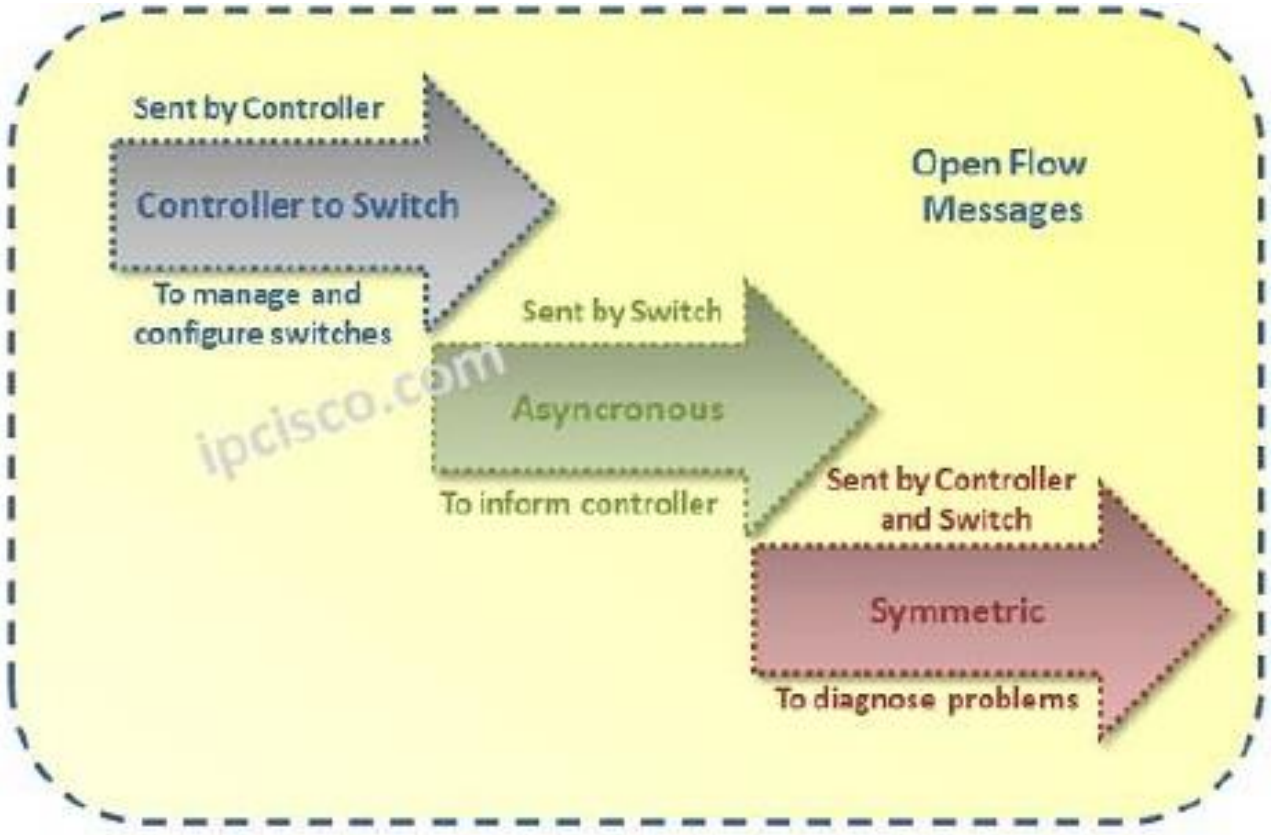
PARTIE 2

OpenFlow Messages

- n

OpenFlow Messages

- Le protocole OpenFlow supporte trois types de messages :



OpenFlow Messages

Contrôleur-vers-Switch

- Ces messages sont initiés par le contrôleur et utilisé pour inspecter ou gérer directement l'état du Switch
- Peuvent ou peuvent ne pas nécessiter une réponse de la part du Switch
    - **Features** : le contrôleur demande et reçoit l'identité et les fonctionnalités de base du Switch. Cet échange est généralement effectué après l'établissement du canal OpenFlow
    - **Configuration** : requête de configuration ou de lecture de configuration
    - **Modify-State** : gérer l'état du Switch (ajouter, modifier ou supprimer des entrées des tables de flux/groupes, modifier les propriétés des ports du Switch)
    - **Read-State** : pour collecter des information sur les Switchs (configuration courante, statistiques ou caractéristiques)
    - **Packet-out** : pour envoyer un paquet à partir d'un port du Switch
    - **Barrier** : mécanisme permettant d'être informé du moment de la fin d'exécution d'un message
    - **Role-Request** : le contrôleur envoi ce message quand il décide de changer de rôle

OpenFlow Messages

Messages asynchrones :

- ils sont envoyés du Switch vers le contrôleur pour notifier l'arrivé d'un paquet, le changement de l'état du Switch ou une erreur :
  - **Packet-in** : transporte des paquets transmis au port réservé du contrôleur utilisant une entrée de table de flux ou de table-miss
  - **Flow-Removed** : informe le contrôleur de la suppression d'une entrée de la table de flux (**flag OFPFF_SEND_FLOW_REM**) suite à une requête du contrôleur ou à une expiration du timeout du flux
  - **Port-Status** : informe le contrôleur d'un changement au niveau d'un port (changement de configuration : p.ex. par un utilisateur ou changement d'état : p.ex. liaison down)
  - **Error** : par ces messages, le Switch est capable de notifier au contrôleur tout type de problème

Messages symétriques :

- ils sont envoyés sans sollicitation dans les deux sens :
  - **Hello** : les messages HELLO sont échangés entre le Switch et le contrôleur après l'initiation de la connexion
  - **Echo** : Echo Request/Reply sont utilisés pour vérifier qu'une connexion (Contrôleur-Switch) est encore en vie; Ils sont utilisés également pour mesurer la latence ou la bande passante
  - **Experimenter** : destinés à tester des fonctionnalités supplémentaire de manière standardisée (usage futur)

OpenFlow Messages

- ,,

Message Category	Message	Message Type	Direction	Process
Conf.	Hello	Symmetric	Controller->Switch	"Here is my Version Number!"
	Hello	Symmetric	Switch->Controller	"Here is Verision Number, that I support!"
	Features Request	Control/Switch	Controller->Switch	"Which ports are available?"
	Set Config	Control/Switch	Controller->Switch	"Could you send Flow Expirations?"
	Features Reply	Control/Switch	Switch->Controller	"Here are the available ports / supported actions!"
	Port Status	Asynchronous	Switch->Controller	Informing Controller about some features.
Flow	Packet-In	Asynchronous	Switch->Controller	"There is no match in Flow Table for this Flow!"
	Packet-Out	Control/Switch	Controller->Switch	"Send packet out to these ports!"
	Flow-Mod	Control/Switch	Controller->Switch	"Add this Flow to the Flow Table!"
	Flow-Expired	Control/Switch	Switch->Controller	Flow timed out after being inactive for a period.

© By Gokhan Kosem, www.ipcisco.com

PARTIE 2

CHAPITRE 3

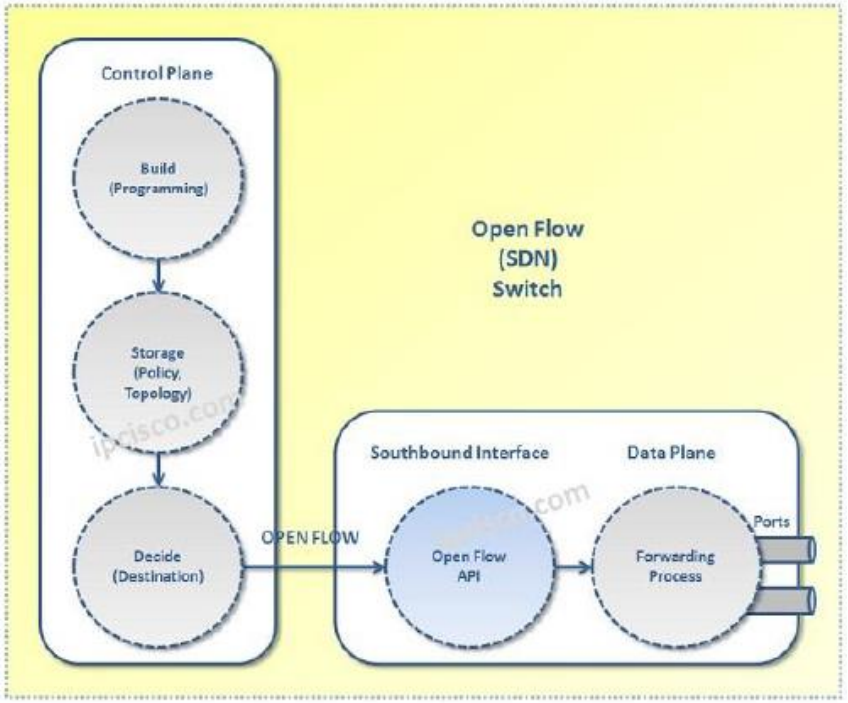
Etudier le protocole OpenFlow

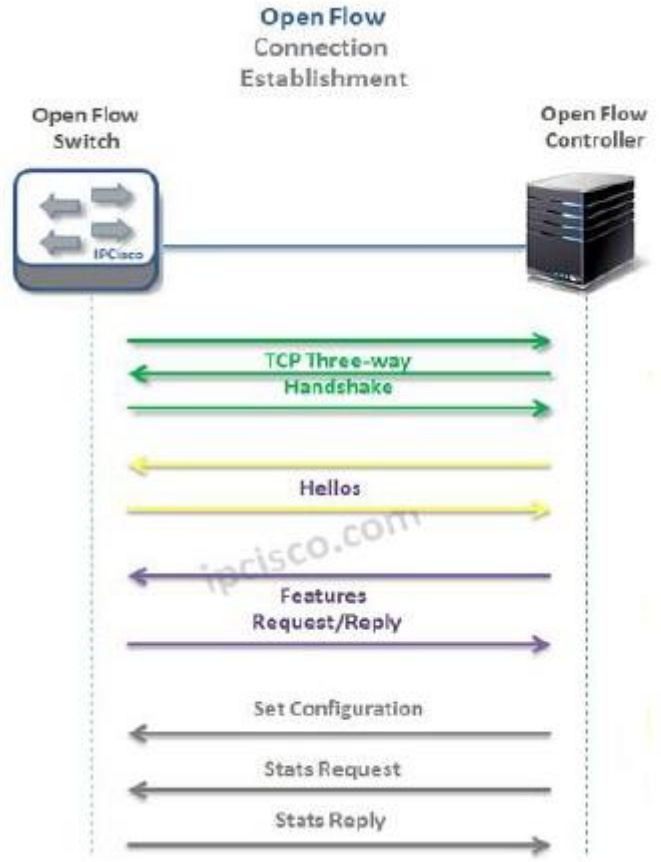
1. Présentation du protocole OpenFlow
2. Flow Table et Les messages Openflow
3. OpenFlow Switches
4. Architecture et le fonctionnement du contrôleur

PARTIE 2

Les Switchs OpenFlow

- „





Les Switchs OpenFlow

- **Hardware-based OpenFlow Switches**
  - Commutateurs matériels commerciaux avec capacité OpenFlow
  - Afficher une vitesse de traitement élevée
  - Avoir une limitation d'espace pour enregistrer les entrées de la table de flux (en raison de la CAM coûteuse)
  - Pas facile à mettre à niveau
- **Software-based OpenFlow Switches**
  - Commutateur logiciel compatible OpenFlow (fonctionne sur un ordinateur standard x86)
  - Les performances sont relativement faibles
  - Stocker une grande quantité d'entrées de flux
  - En cours de développement actif, prend en charge les spécifications OpenFlow les plus récentes.
- **Hybrid OpenFlow Switch**
  - Un commutateur virtuel avec un périphérique matériel spécialisé
  - Plus rapide que les commutateurs logiciels

Hardware-based OpenFlow Switches

- Arista 7050
- Brocade MLXe, Brocade CER, Brocade CES
- Extreme Summit x440, x460, x670
- Huawei openflow-capable router platforms
- HP 3500, 3500yl, 5400zl, 6200yl, 6600, and 8200zl (the oldstyle
- L3 hardware match platform)
- HP V2 line cards in the 5400zl and 8200zl (the newer L2
- hardware match platform)
- IBM 8264
- Juniper (MX, EX)
- NEC IP8800, NEC PF5240, NEC PF5820
- NetGear 7328SO, NetGear 7352SO
- Pronto (3290, 3295, 3780) - runs the shipping pica8 software

Software-based OpenFlow Switches

- **Indigo:** Implémentation open source qui s'exécute sur des commutateurs physiques et utilise les fonctionnalités des ASIC pour exécuter OpenFlow
- **LINC:** Implémentation open source qui s'exécute sur Linux, Solaris, Windows, MacOS et FreeBSD
- **Pantou:** Transforme un routeur/point d'accès sans fil commercial en un commutateur compatible OpenFlow. Prend en charge Broadcom générique et certains modèles de points d'accès LinkSys et TP-Link avec les chipsets Broadcom et Atheros.
- **Of13softswitch:** Commutateur logiciel d'espace utilisateur basé sur le commutateur logiciel Ericsson TrafficLab 1.1
- **XORPlus:** Logiciel de commutation open source pour piloter des ASIC hautes performances. Prend en charge STP/RSTP/MSTP, LCAP, QoS, VLAN, LLDP, ACL, OSPF/ECMP, RIP, IGMP, IPv6, PIM-SM
- **OpenvSwitch:** Commutateur virtuel open source

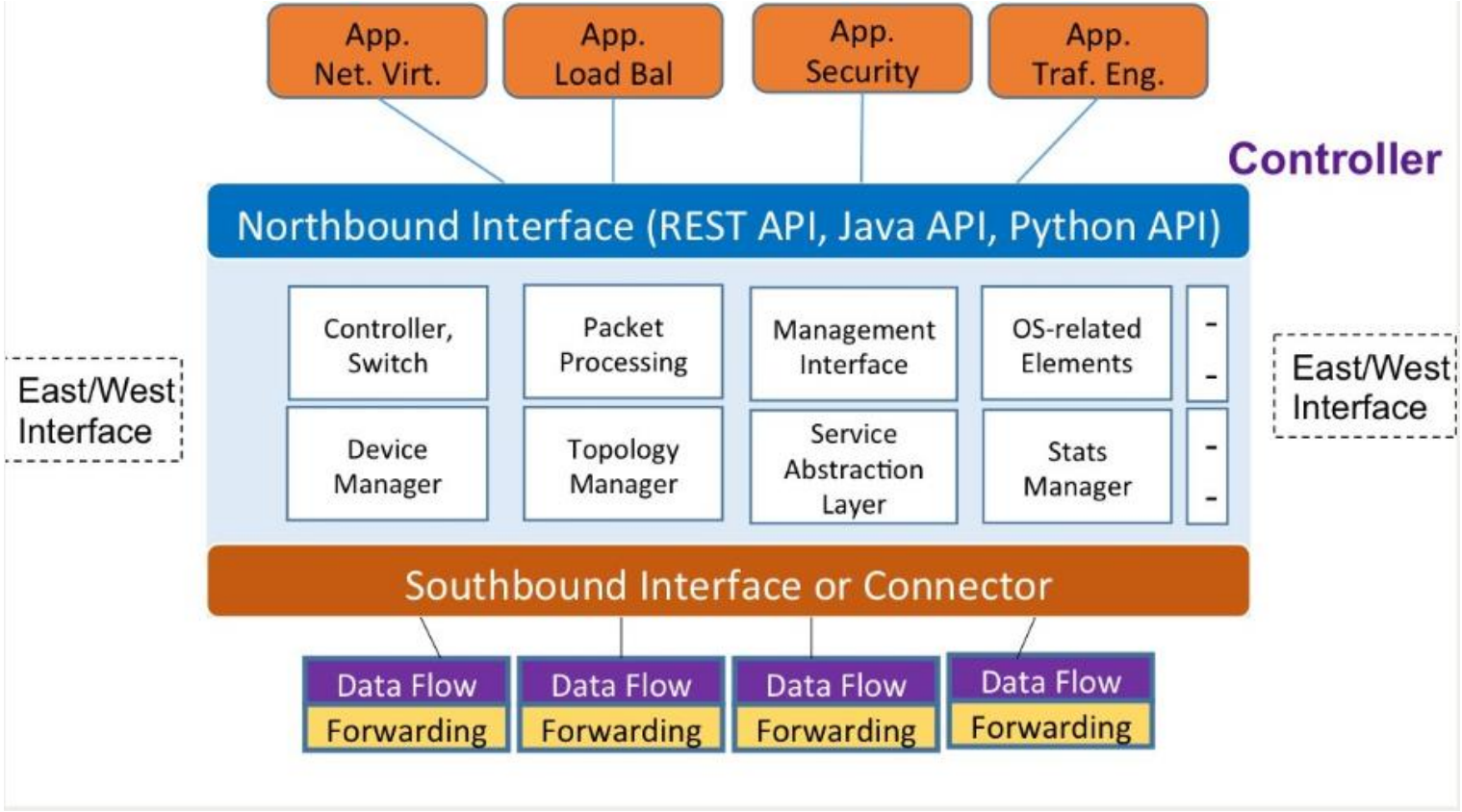
CHAPITRE 3

Etudier le protocole OpenFlow

1. Présentation du protocole OpenFlow
2. Flow Table et Les messages Openflow
3. OpenFlow Switches
4. Architecture et le fonctionnement du contrôleur

PARTIE 2

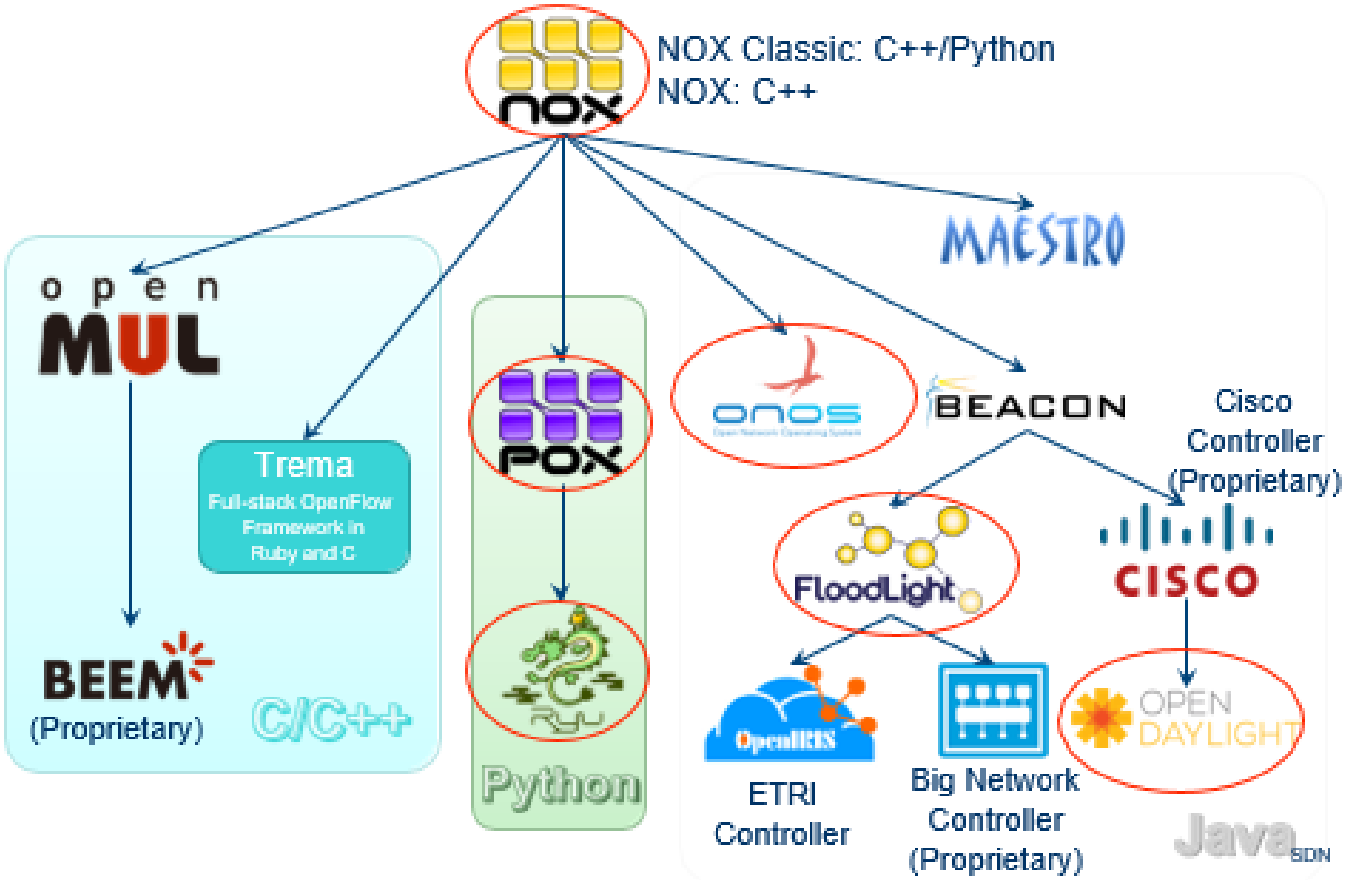
Composants du contrôleur SDN



PARTIE 2

Contrôleur SDN

- **OpenFlow Controllers**
- NOX
- POX
- Beacon
- Floodlight
- Ryu
- OpenDaylight
- Open Network Operating System (ONOS)



NOX

- L'un des premiers contrôleurs open source OpenFlow
- Développé par Nicira et donné à la communauté de la recherche en 2008
- Soutenu par ON.LAB à Stanford et par UC Berkeley
- Fournit une API C++ pour OpenFlow 1.0
- À la fois un contrôleur et un framework pour développer des applications OpenFlow
- Comprend des exemples de composants pour la découverte de la topologie, le commutateur d'apprentissage et le commutateur à l'échelle du réseau
- NOX a été développé par CPqD pour prendre en charge OpenFlow 1.3 en novembre 2012

POX

- Nouvelle version de NOX basée sur Python.
- Plate-forme de développement rapide de logiciels de contrôle de réseau à l'aide de Python
- Contrôleur OpenFlow plus un cadre pour interagir avec les commutateurs OpenFlow, le débogage, la virtualisation du réseau, ...
- Composants réutilisables pour la sélection de chemin, la découverte de la topologie
- Fonctionne sous Linux, MAC OS, Windows
- Peut être fourni avec le runtime PyPy sans installation pour un déploiement facile

NOX/POX

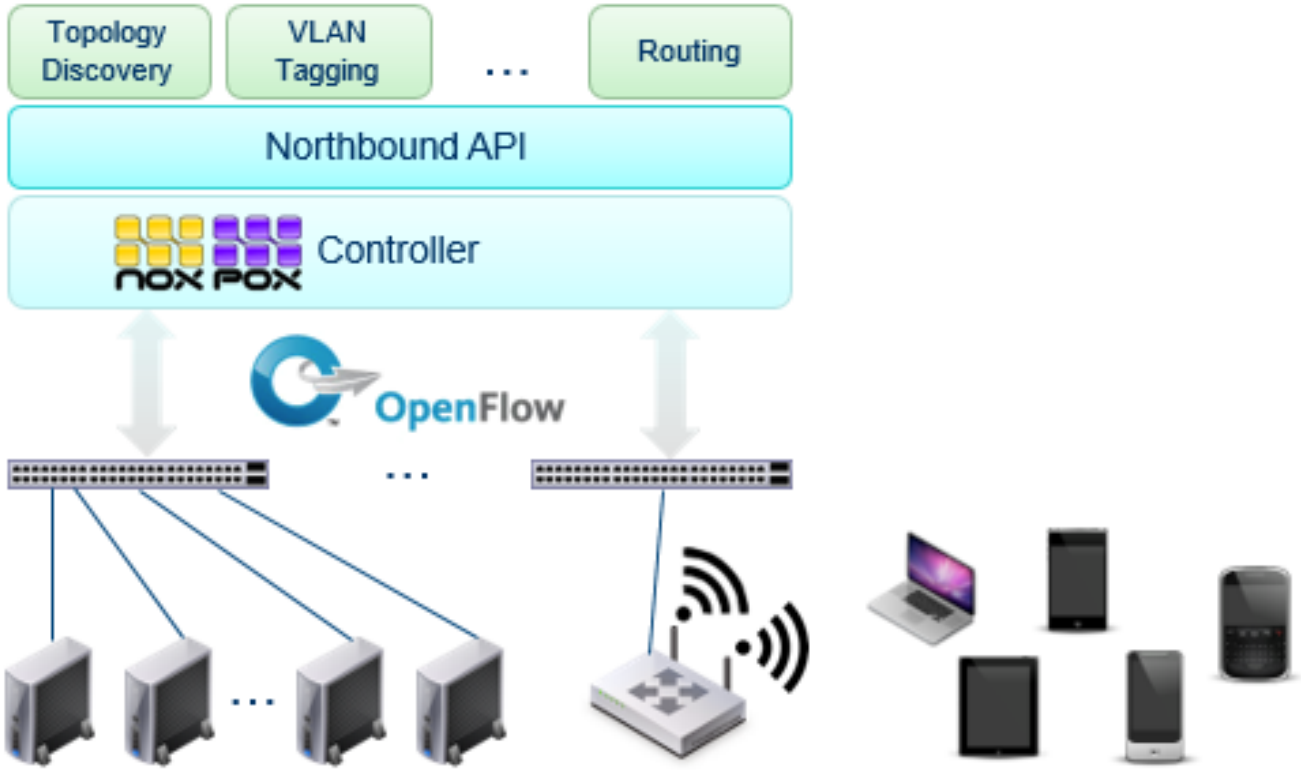
Network Application Services
- Nouvelles fonctions en tant que services logiciels

Northbound API
- Fournir une interface aux applications réseau
- Pas encore normalisé

- **NOX/POX Controller – Network OS**
  - Fournir des abstractions à l'échelle du système
  - Transformer la mise en réseau en un problème logiciel

Southbound API
- Protocole OpenFlow standardisé
- Contrôleur, interopérabilité des commutateurs

- **OpenFlow Enabled Switches**
  - Nouvelles fonctions en tant que services logiciels



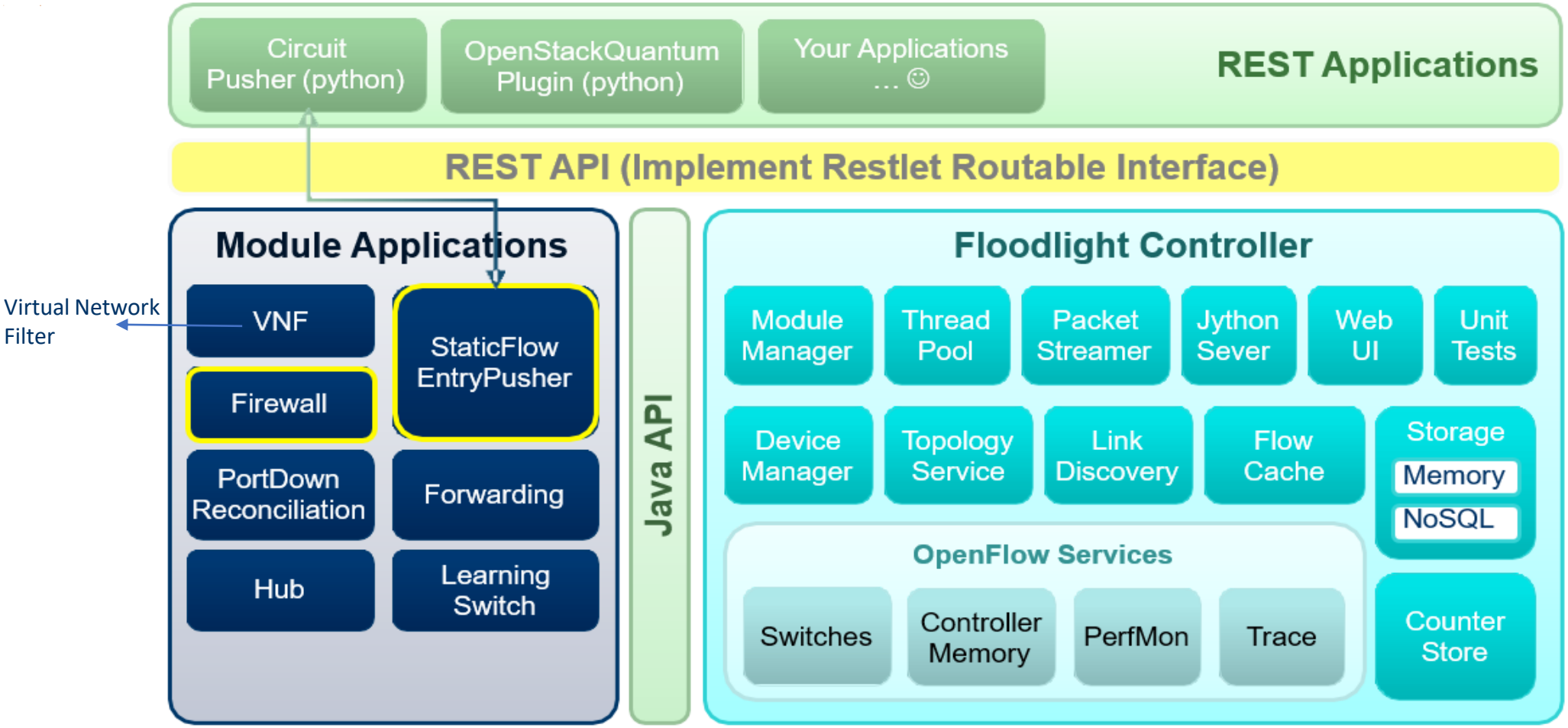
PARTIE 2

Floodlight

- Contrôleur OpenFlow basé sur Java basé sur Beacon
- Fonctionne avec des commutateurs physiques et virtuels qui utilisent le protocole OpenFlow
- **Open source** : Floodlight est développé par une communauté ouverte de développeurs.
- **Facile à utiliser** : Floodlight est simple à construire et à exécuter.
- **Testé et pris en charge** : Floodlight est activement testé et amélioré par une communauté de développeurs professionnels

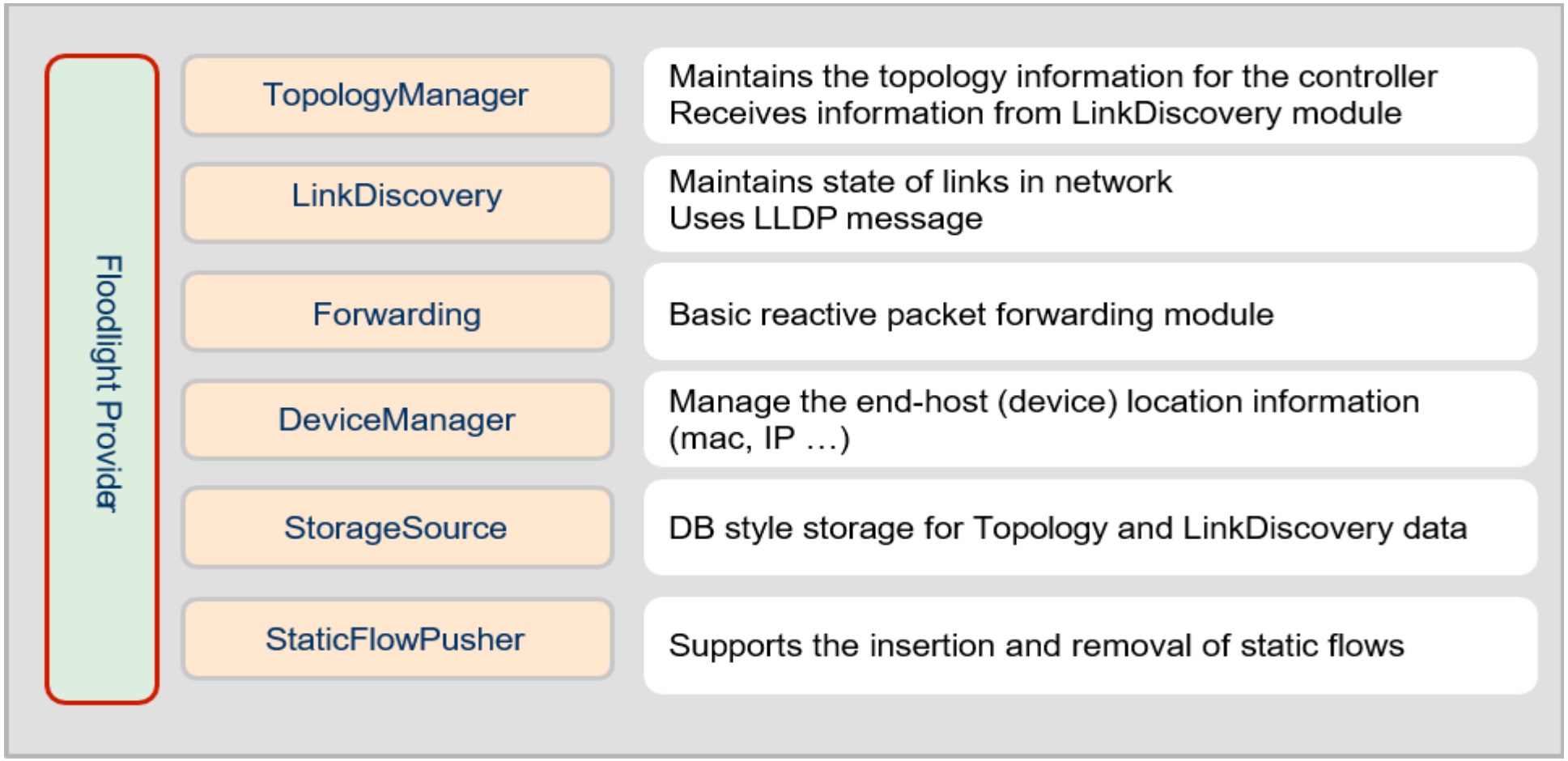
PARTIE 2

Architecture de Floodlight



PARTIE 2

Description des modules

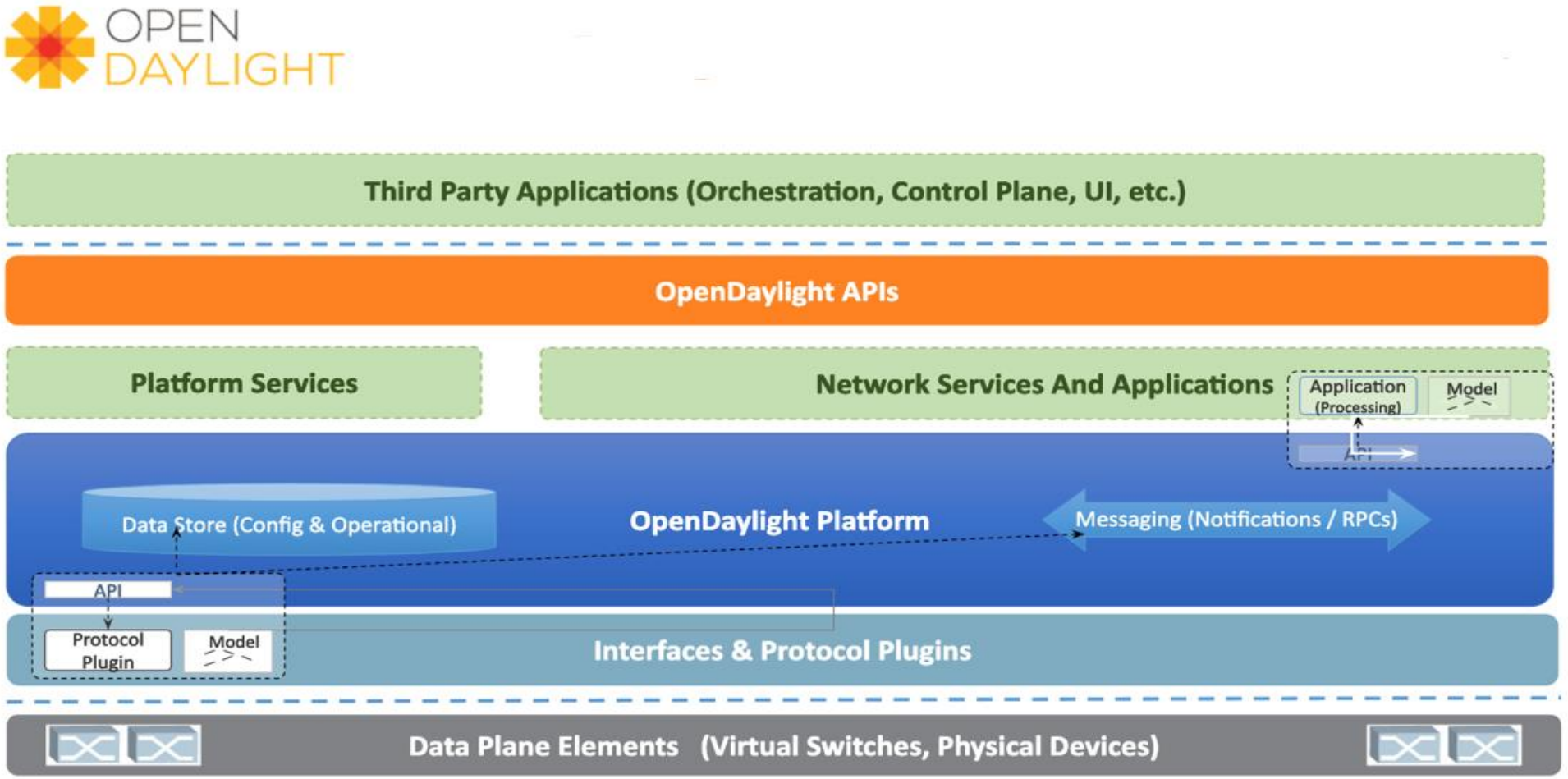


OpenDylight

- Le projet OpenDaylight (ODL) est une plate-forme collaborative et open source pour accélérer l'adoption et l'innovation de la mise en réseau logiciel (SDN) et de la visualisation des fonctions réseaux (NFV).
- ODL est un logiciel basé sur Java et pris en charge par l'industrie, géré par le consortium Linux Foundation avec près de 50 entreprises membres, dont Brocade, Cisco, Citrix, Dell, Ericsson, HP, IBM, Juniper, Microsoft et Red Hat.
- La mission d'ODL est de créer une communauté collaborative qui partage et contribue au succès et à l'adoption du SDN.
- Il contient un contrôleur modulaire et souple.
    - Modularité et extensibilité à exécution
    - Multiprotocol au niveau bas
    - Couche d'abstraction des services
    - Support du Multi-tenant/Découpage

PARTIE 2

Architecture OpenDylight



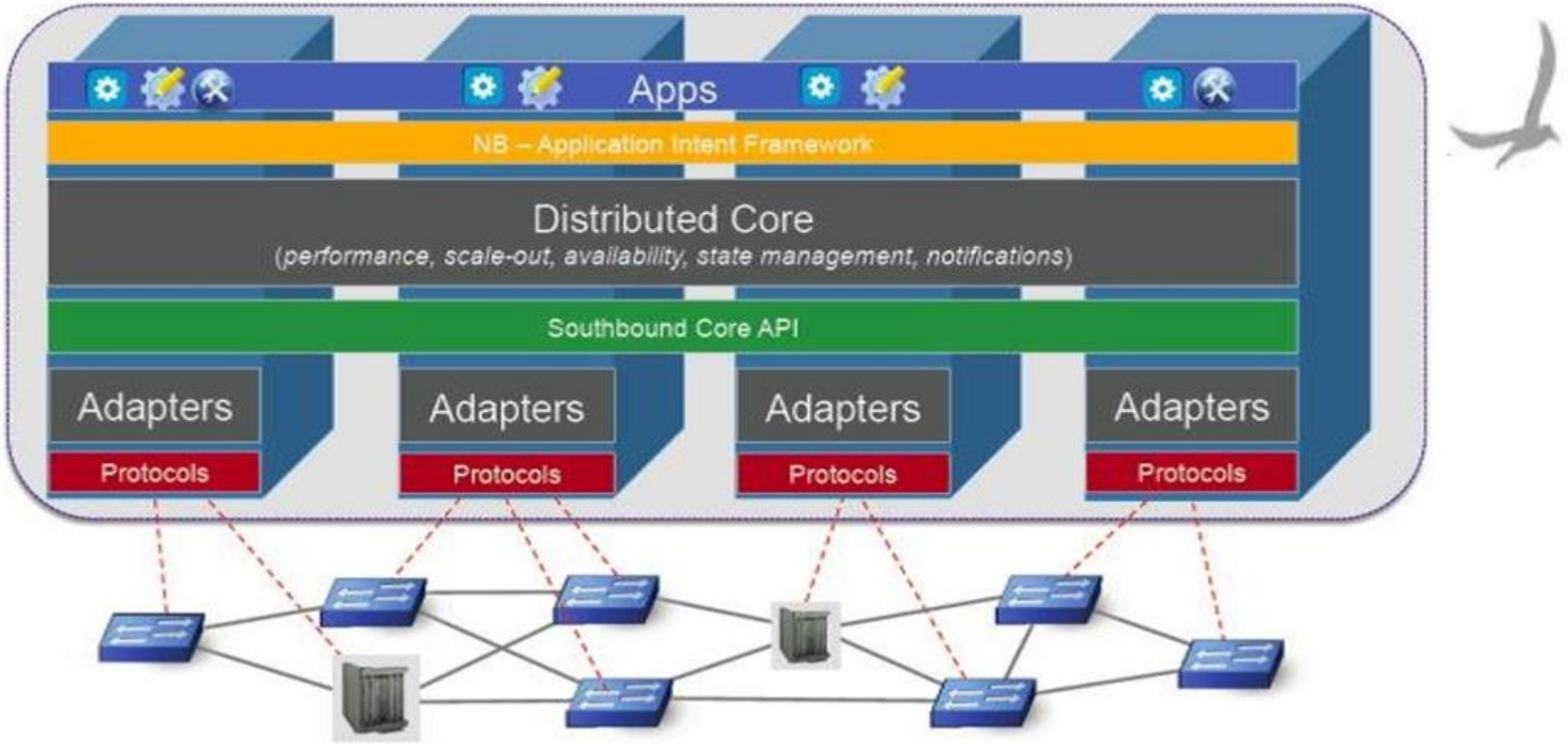
PARTIE 2

ONOS

- Open Network Operating System (ONOS®) est le principal contrôleur SDN open source pour la création de solutions SDN/NFV de nouvelle génération.
- ONOS a été conçu pour répondre aux besoins des opérateurs souhaitant créer des solutions de classe opérateur qui tirent parti de l'économie du matériel en silicium marchand tout en offrant la flexibilité nécessaire pour créer et déployer de nouveaux services de réseau dynamiques avec des interfaces de programmation simplifiées.
- ONOS prend en charge à la fois la configuration et le contrôle en temps réel du réseau, éliminant ainsi le besoin d'exécuter des protocoles de routage et de contrôle de commutation à l'intérieur de la structure du réseau.
- En déplaçant l'intelligence dans le contrôleur cloud ONOS, l'innovation est activée et les utilisateurs finaux peuvent facilement créer de nouvelles applications réseau sans avoir à modifier les systèmes de plan de données.
- La plateforme ONOS comprend :
  - Une plate-forme et un ensemble d'applications qui agissent comme un contrôleur SDN extensible, modulaire et distribué.
  - Gestion, configuration et déploiement simplifiés de nouveaux logiciels, matériels et services.
  - Une architecture évolutive pour fournir la résilience et l'évolutivité requises pour répondre aux rigueurs des environnements de production des opérateurs.

PARTIE 2

Architecture ONOS



CHAPITRE 3

Assurer la sécurité des réseaux SDN

Ce que vous allez apprendre dans ce chapitre :

- La sécurité OpenFlow

6 heures

CHAPITRE 3

Assurer la sécurité des réseaux SDN

1. Disponibilité dans la spécification OpenFlow
2. Contrôle d’accès
3. Intégrité

Specifications

- OpenFlow version 0.8.9 (2 décembre 2008) : Comportement défini lorsque la connexion du contrôleur est perdue ("ne rien faire - laisser les flux expirer naturellement", "geler les délais", "devenir un commutateur d'apprentissage" et "tenter de se connecter à un autre contrôleur")
- OpenFlow version 0.9 (20 juillet 2009) : la première version qui inclut un mécanisme de basculement simple

  Cache de flux d'urgence : entrées de flux spécifiques aux urgences qui sont inactives jusqu'à ce qu'un commutateur perde la connectivité du contrôleur
- OpenFlow version 1.0 (31 décembre 2009) : remplacer les références SSL par TLS
- OpenFlow version 1.1 (28 février 2011) :

  Supprimer le cache de flux d'urgence de la spécification en raison du manque d'adoption et de la complexité à mettre en œuvreLes déclencheurs d'interruption de connexion échouent en mode sécurisé ou autonome.

  En mode sécurisé, le commutateur continue de fonctionner en mode OpenFlow jusqu'à ce qu'il se reconnecte à un contrôleur.

  En mode autonome en cas d'échec, le commutateur revient à l'utilisation du traitement normal (commutation Ethernet)
- OpenFlow version 1.2 (5 décembre 2011) :

  Mécanisme de changement de rôle du contrôleur : permet à chaque contrôleur de changer ses rôles en égal, maître ou esclave
- OpenFlow Version 1.4.0, le message d'état du rôle permet au commutateur d'informer le contrôleur du changement de son rôle

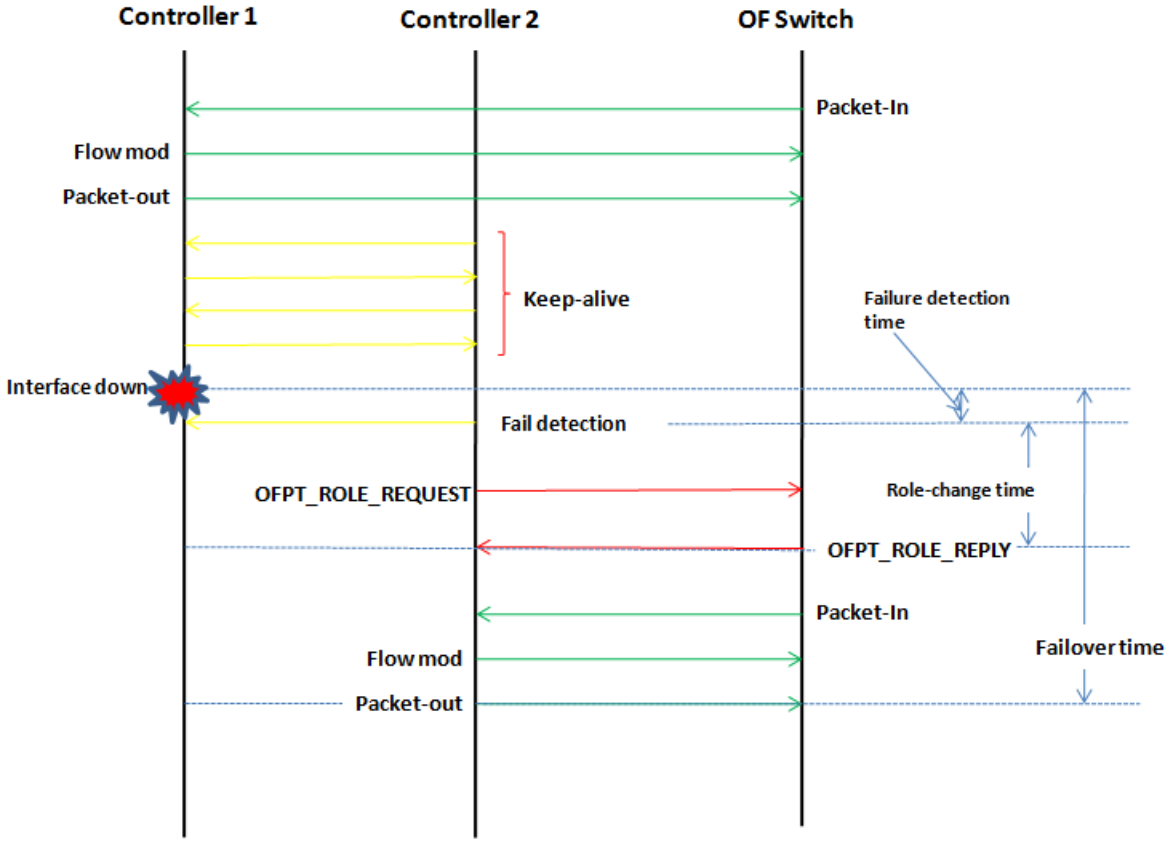
Disponibilité dans la spécification OpenFlow

- Disponibilité dans la spécification OpenFlow
  - Load Balancing / Failover
  - Load Balancing : EQUAL / EQUAL or MASTER / EQUAL
  - Failover : MASTER / SLAVE
- Messages spécifiques : ***OFPT_ROLE_REQUEST***, ***OFPT_ROLE_REPLY***

Role field of « OFPT_ROLE_REQUEST"		
0	OFPCR_ROLE_NOCHANGE	Pas de changement de rôle
1	OFPCR_ROLE_EQUAL	Rôle par défaut : Full access
2	OFPCR_ROLE_MASTER	Au maximum, un Master: Full access
3	OFPCR_ROLE_SLAVE	Read Only access

Disponibilité dans la spécification OpenFlow

- Scénario de Failover



PARTIE 2

PARTIE 2

Disponibilité dans la spécification OpenFlow

- **Performance**

- OpenFlow 1.5.0 (depuis1.4.0 version)
  - Mécanisme d'éviction (mesure corrective)
    - Quand la table de flux est saturée, de nouvelle règles de flux ne
    - peuvent êtres ajoutées et un message d'erreur est retourné au contrôleur
    - Le mécanisme d'éviction permet au Switch de supprimer automatiquement des entrés de flux moins importantes pour créer suffisamment d'espace pour en rajouter de nouvelles
    - Atténue les dégradations de performances dans les situations extrêmes
  - Vacancy Event (mesure préventive)
    - Grace aux ***Vacancy events***, le contrôleur reçoit une alerte quand la table de flux atteint un seuil de remplissage prédéfini
    - Le contrôleur anticipe à l'avance les situations de saturation et agit pour résoudre le problème

- **Fonctionnalité « Group table »**

- Monitoring permanent de l'état des ports des Switchs
  - La valeur du champ ***OFPPC_PORT_DOWN*** du message ***ofp_port_config*** communique l'état du port au contrôleur
  - La valeur du champ ***OFPPC_LINK_DOWN*** du message ***ofp_port_state*** communique l'état du lien au contrôleur
- L'exploitation de ***Fast Failover Table Group (chemin de backup précalculé)*** permet de renseigner le Switch sur le comportement en cas de panne de port ou de lien de façon autonome (sans revenir au contrôleur)

PARTIE 2

Disponibilité Fast Failure Recovery

AFRO (Automatic Failure Recovery for OpenFlow) – La problématique de la reprise après un échec d'un **élément du réseau** (Switch en l'occurrence)

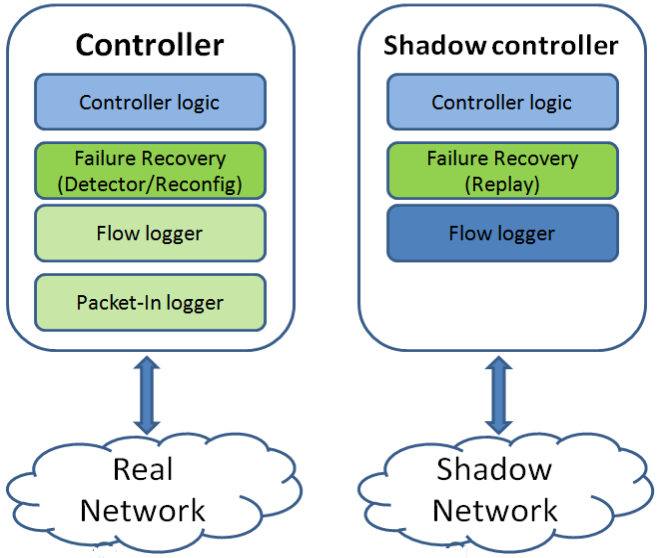
- ✓ Automatisation de la reprise après incidents de réseau SDN
- ✓ Idée principale : Séparation des modules fonctionnels de ceux relatifs à la reprises après échec
  - Réduit la probabilité d'introduction de bugs dus à la complexité des modules développés
- ✓ ***Shadow Controller*** : Après détection d'échec d'un composant réseau, créer un contrôleur logique travaillant sur un environnement émulé identique mais sans le noeud en échec
  - Re-calcul de l'état de transmission de nouvelle topologie (peut être effectué avant l'incident pour accélérer la reprise)
- ✓ AFRO opère en deux modes :

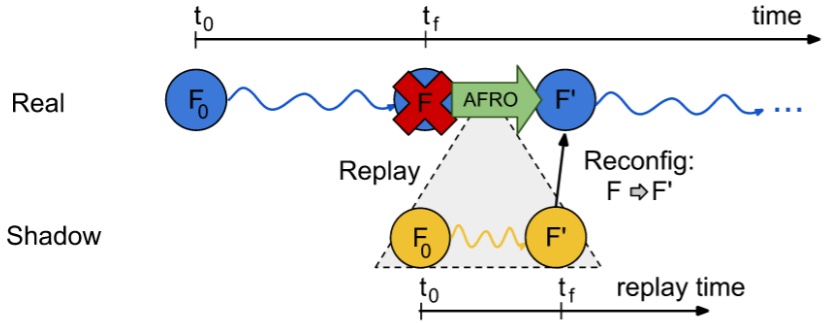
Record mode : Etat normal du réseau

Enregistre tous les ***PacketIn*** et garde trace des règles configurées « ***FlowMod*** » et « ***FlowRem*** »

Recovery mode : activé après la découverte d'un échec (Replay + Reconfig)

- **Replay** : AFRO crée une nouvelle instance du contrôleur « shadow controller » identique mais avec un état de transmission vierge
- **Reconfiguration** : Application des changements de configuration au niveau du contrôleur et des Switchs sans mettre le réseau dans un état inconsistant. Deux étapes à distinguer :





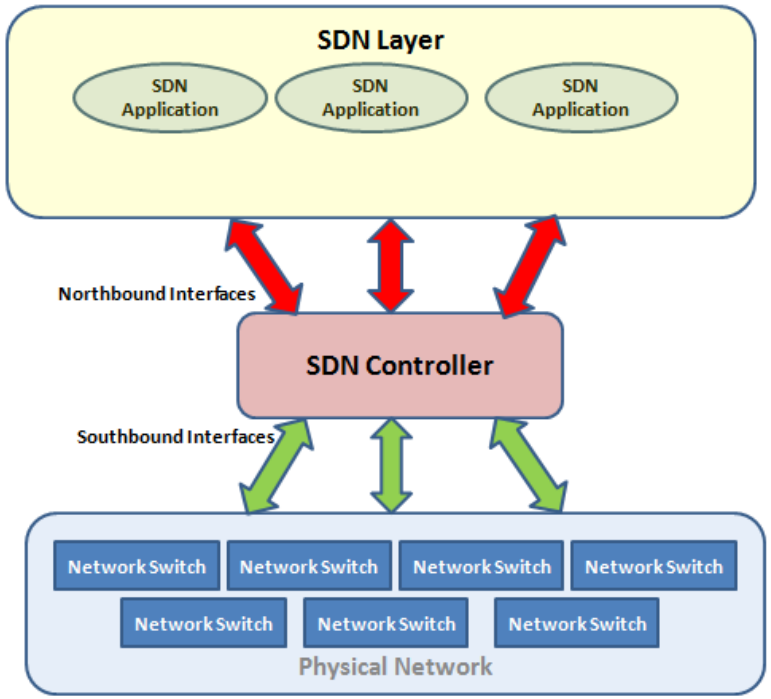
CHAPITRE 3

Assurer la sécurité des réseaux SDN

1. Disponibilité dans la spécification OpenFlow
2. Contrôle d’accès
3. Intégrité

Disponibilité : Fast Failure Recovery

- Privilèges élevés du contrôleur sur les Switchs
  - Peut être exploités à des fins malveillantes
- Deux types d'interfaces d'accès au contrôleur :
  - Southbound interface (Switch au contrôleur)
  - Northbound interface (application au contrôleur) : **la sécurité de cette interface est hor périmètre de la spécification OpenFlow**



Sécurité de l'interface Northbound

- Il s'agit de l'interface qui permet la programmabilité du contrôleur
- La stratégie de contrôle d'accès doit être la plus restrictive possible pour empêcher les effets d'erreurs ou d'introduction d'applications malicieuses
- Stratégie « defense in depth » :
  - Verrouiller le contrôleur autant que possible
  - Désactiver les comptes et les services non nécessaires
  - Maintenir le contrôleur à jour (correction des vulnérabilités)
  - **Politique de gestion des droits en conformité avec les principes fondamentaux de la sécurité (Least privilege & separation of duties)**
  - Monitoring permanent de l'activité des ressources critiques (CPU, RAM, I/O…)
  - Journalisation des activités critiques
  - Surveiller toute déviation par rapport à un profil de comportement normal (IDS)
  - Profils ***fail safe*** vs ***fail secure***
  - …

Sécurité de l'interface Southbound

- Southbound interface (network devices to controller)
  - Problématique essentielle : Authentification entre le Switch et le contrôleur
  - **« The OpenFlow channel is usually encrypted using TLS, but may be run directly over TCP "**
- L'usage de TLS assure :
  - L'authentification du contrôleur (requise)
  - L'authentification du noeud réseau par certificat (optionelle)
  - La confidentialité des données échangées (session chiffrée)
  - L'intégrité des données échangées
- Points critiques :
  - L'usage de TLS est optionnel jusqu'à la version 1.5.0
  - Pas de mention sur la version de TLS
  - La version 1.5.1 (Mars 2015) recommande l'usage de la version 1.2 de TLS
  - Pas de précision sur la version du certificat à utiliser pour l'authentification
- Apports de TLS 1.2
  - Correction de la vulnérabilité Mant-In-The-Middle Attack (CBC attack)
  - Remplacement des algorithmes MD5/SHA1 par SHA256
  - Compatibilité avec SSL 2.0 n'est plus obligatoire

CHAPITRE 3

Assurer la sécurité des réseaux SDN

1. Disponibilité dans la spécification OpenFlow
2. Contrôle d’accès
3. Intégrité

PARTIE 2

Sécurité

- Le contrôleur est supposé interagir avec plusieurs types d'applications
- Possibilité de conflits entre les règles générées par diverses applications
- Catégorisation des applications par rôle:
  - **ADMIN** : politique statique définie par l'administrateur
  - Politique Firewall, zoning réseau, ACL
  - **SEC-APP** : application générant des règles dynamiques en réponse à des événements précis NAC, DLP, IPS…
  - **APP** : applications classiques d'ingénierie de trafic : routage, QoS, Load balancing…
- **RCA** : Rule-Based Conflict Analysis
- Champ d'application : Couche application vers Couche infrastructure
- Concerne les messages d'ajout ou de modification de règle de flux (***Flow rule Mod***) et concerne tous les types d'applications

Politique : ***aucune application d'un niveau de privilège déterminé ne doit ajouter une règle de flux en conflit avec une autre ajoutée par une application de niveau de privilège supérieur***

Exemple : une application de routage autorise un flux qui a été bloqué par une application IPS

PARTIE 2

Politique de médiation

- **RCA** : Rule-Based Conflict Analysis
  - Champ d'application : Couche application vers Couche infrastructure
  - Concerne les messages d'ajout ou de modification de règle de flux (***Flow rule Mod***) et concerne tous les types d'applications

  Politique : ***aucune application d'un niveau de privilège déterminé ne doit ajouter une règle de flux en conflit avec une autre ajoutée par une application de niveau de privilège supérieur***
- Exemple : une application de routage autorise un flux qui a été bloqué par une application IPS
- **Public read** : concerne les messages des événements notifiés par les noeuds réseaux aux applications (n'affectent pas les tables de flux)
  - **Global Read** : les événements destinés à toutes les applications
    - Flow removal messages, flow error reply …
  - **Selected Read** : les événements destinés uniquement à certaines applications concernées par l'événement

    Barrier replies, Packet-In return, Switch config reply, Switch stats report and Echo replies

  Politique : ***conformité au principe Least privilege par la limitation de la visibilité des applications sur le réseau au strict minimum nécessaire***
- **Permission *:*** opérations spécifiques nécessitant une permission explicite avant d'être autorisées
  - Configuration de switchs ou tests de connectivité (peuvent altérer les règles de flux ou la configuration des Switchs)
  - Barrier request, Packet-Out, Switch port mod, Switch port status, Switch set config, Switch get config, Switch stats request, Echo request, Vendor features, vendor actions

  Politique : ***conformité au principe Least privilege par la limitation des privilèges sur le réseau au strict minimum nécessaire***

Politique de médiation

Flow Direction	Data exchange operation	Mediation Policy	Minimum authorization
Application layer → Infrastructure layer	Flow rule mod	Rule Conflict Analysis	APP
	Barrier requests	Permissions	APP
	Packet-Out	Permissions	SEC
	Switch Port Mod	Permissions	ADMIN
	Switch Set Config	Permissions	ADMIN
	Switch Get Config	Permissions	APP
	Switch Stats request	Permissions	APP
	Echo request	Permissions	APP
	Vendor actions	Permissions	ADMIN
Infrastructure layer →Application layer	Flow removal messages	Global Read	APP
	Flow error reply	Global Read	APP
	Barrier replies	Selected Read	APP
	Packet-In return	Selected Read	APP
	Switch port status	Permissions	ADMIN
	Switch config reply	Selected Read	APP
	Switch stats report	Selected Read	APP
	Echo replies	Selected Read	APP
	Vendor features	Permissions	ADMIN

PARTIE 3

Utiliser les Protocoles

Dans ce module, vous allez :

- Être en mesure de comprendre les politiques de la sécurité dans les environnements SDN
- Être capable de comprendre les mécanismes de la QoS dans les environnements SDN

22 heures

CHAPITRE 1

Garantir la QoS dans les réseaux SDN

Ce que vous allez apprendre dans ce chapitre :

- La QoS dans les réseaux SDN

6 heures

CHAPITRE 2

Garantir la QoS dans les réseaux SDN

1. Avantages de la QoS dans SDN
2. Les solutions QoS pour les réseaux SDN

S

- Supply, provision, measure, control & adapt:

  Delay Jitter Loss Throughput

- Solutions:
  - Hardware: CPU, memory
  - Protocols: routing, queuing, scheduling…
  - Architectures: IntServ, DiffServ, MPLS-TE
- QoS treatments are done hop by hop :
  - Trop de redondance – Difficile à surveiller – Trop de travail pour la reconfiguration – Problèmes d'évolutivité – …
- Network state/statistics collection
- Resource allocation

- Visibilité globale
  - QoS plus affinée
  - Reconfiguration du réseau à tout moment
  - Automatisation de la gestion / personnalisation
  - Programmable
  - Flexible

QoS mechanisms

- Gestion des niveaux de service
- Surveillance de l'état du réseau
- La gestion des ressources
- Routage QoS
- Gestion/contrôle du trafic
  - Classification
    - Identité
    - Marquer
  - Contrôle d'admission/police
    - Compteur
    - (Re-)Marqueur
    - Forme
    - Goutte
  - File d'attente
    - Planification

Défis de QoS dans le SDN

- Point de défaillance unique
- Évolutivité ?

- Surveillance de l'état du réseau

  Charger

  La fréquence

- Configuration des files d'attente
  - Non pris en charge par OpenFlow
  - Fait à chaque saut
- Identification du trafic

CHAPITRE 2

Garantir la QoS dans les réseaux SDN

1. Avantages de la QoS dans SDN
2. Les solutions QoS pour les réseaux SDN

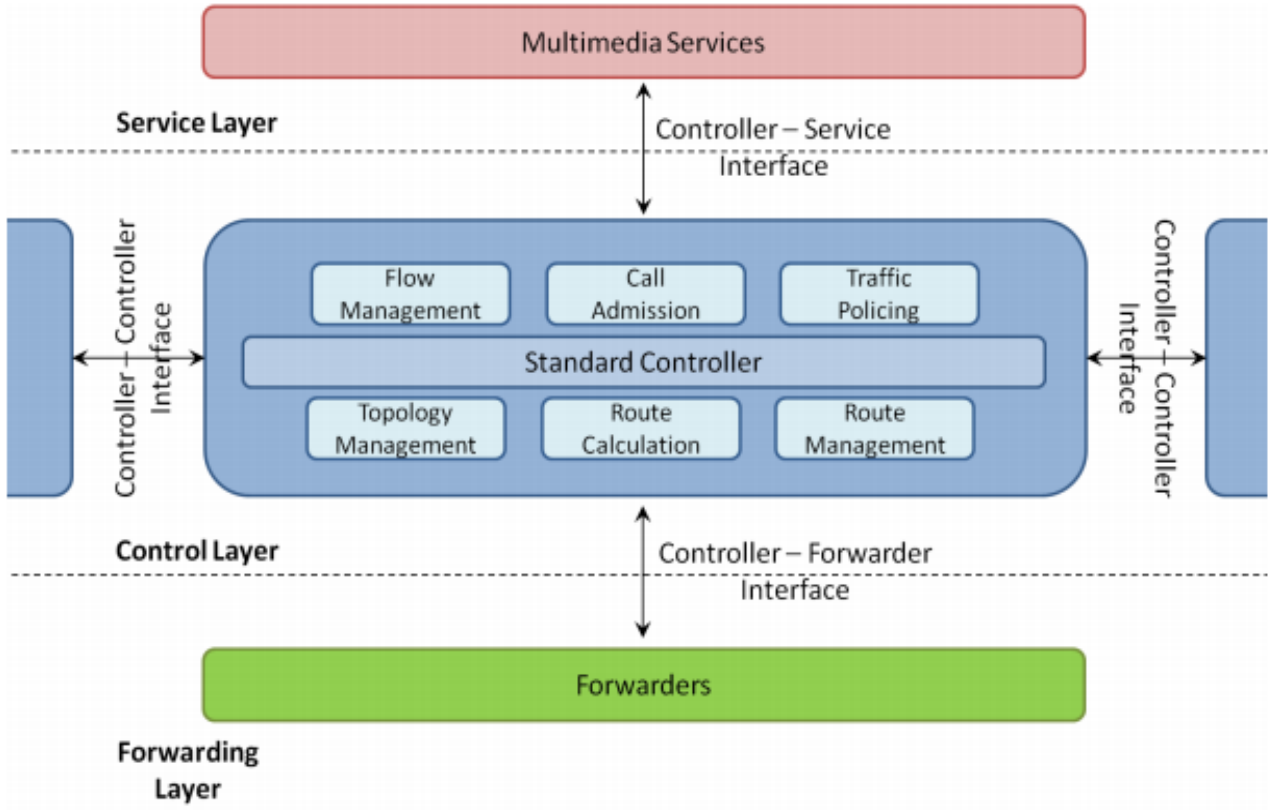
QoS/SDN frameworks

- OpenQoS
- PolicyCop
- FlowQoS
- HiQoS

PARTIE 3

OpenQoS (2012)

- QoS E2E pour les flux multimédia
- Identifier/classer les flux multimédia (IP serveur, DSCP, port, CdS,…)
- Calculer les itinéraires :
  - CSP : chemin le plus court de contrainte
    - Calculer le chemin le plus court en respectant certaines contraintes
    - Coût de l'itinéraire = nombre de sauts + encombrement
    - Contrainte de congestion = le lien dépasse 70 % d'utilisation de sa bande passante
  - SP : chemin le plus court
- Surveillance de l'état du réseau :
  - Périodiquement (1s) recueille des statistiques



❑ **OpenQoS workflow**

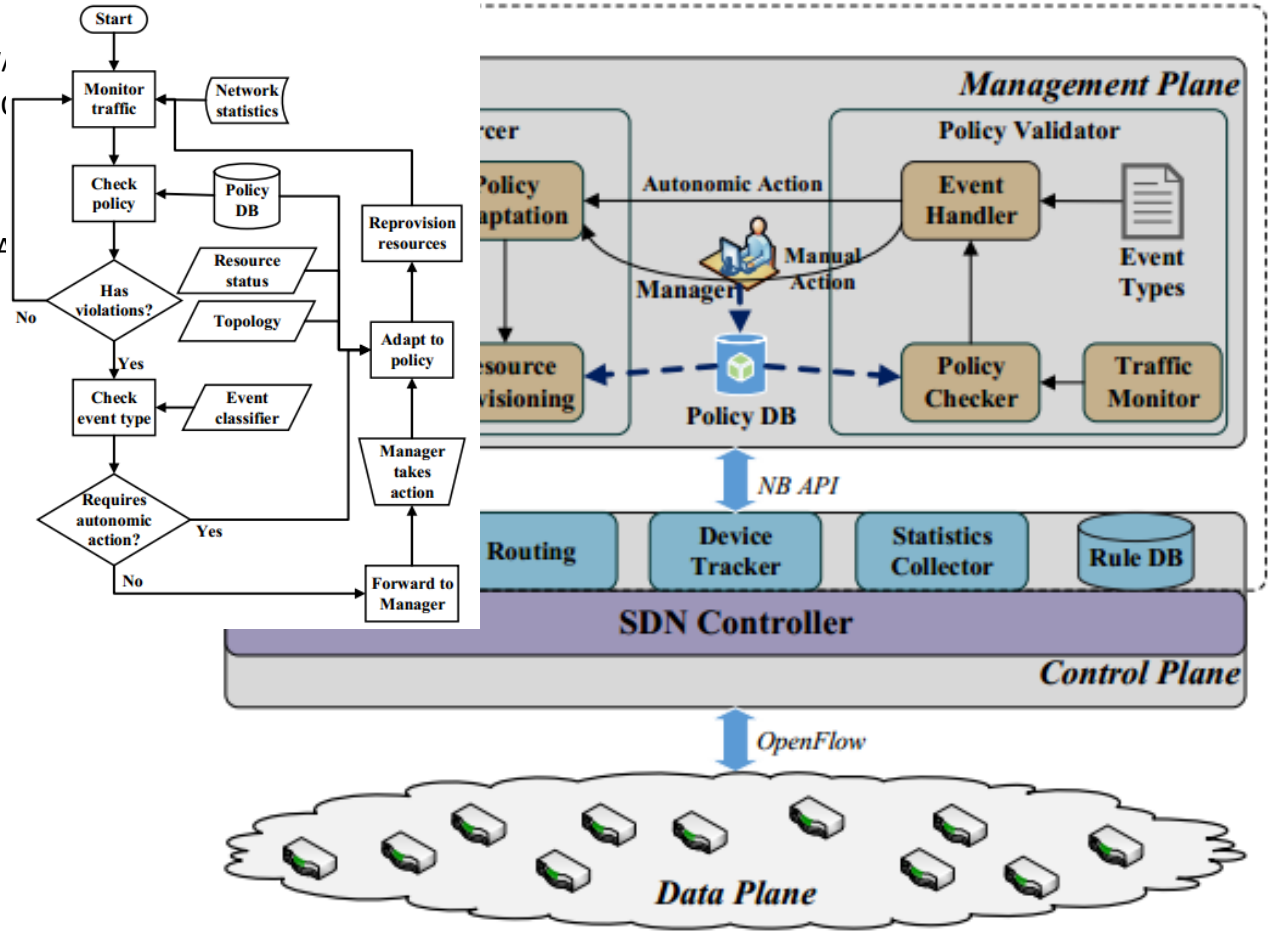
1. Le contrôleur reçoit un nouveau paquet (pkt_in)
2. Vérifier le type de trafic (multimédia ?)
3. Si le paquet est multimédia
   - Calculer le CSP
4. Sinon : calculer SP

PolicyCop (2013)

PolicyCop est un cadre de gestion de politique QoS pour OpenFlow,

- Fournit une interface pour spécifier les SLA basés sur la (
- Applique les SLA via l'API OpenFlow
- Surveille le réseau
- Réajuste les paramètres du réseau pour satisfaire les SLA

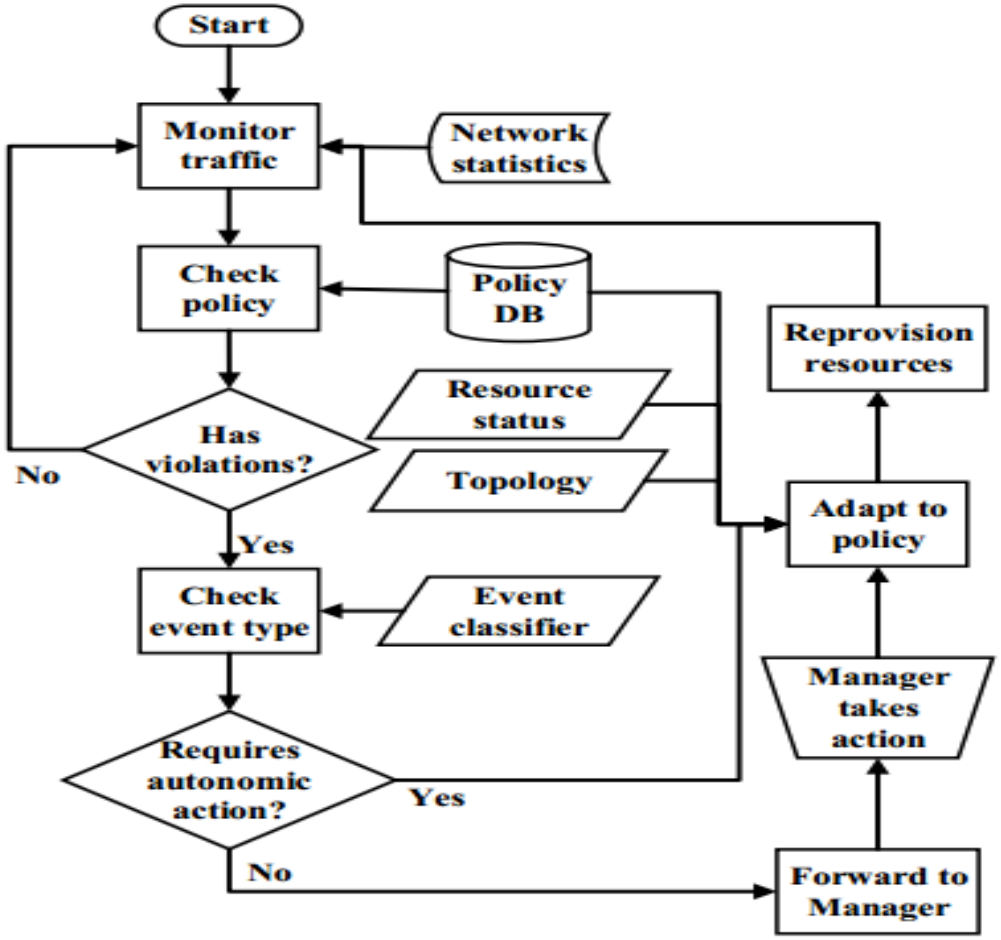
PolicyCop architecture :



PARTIE 3

PolicyCop (2013)

- PolicyCop workflow

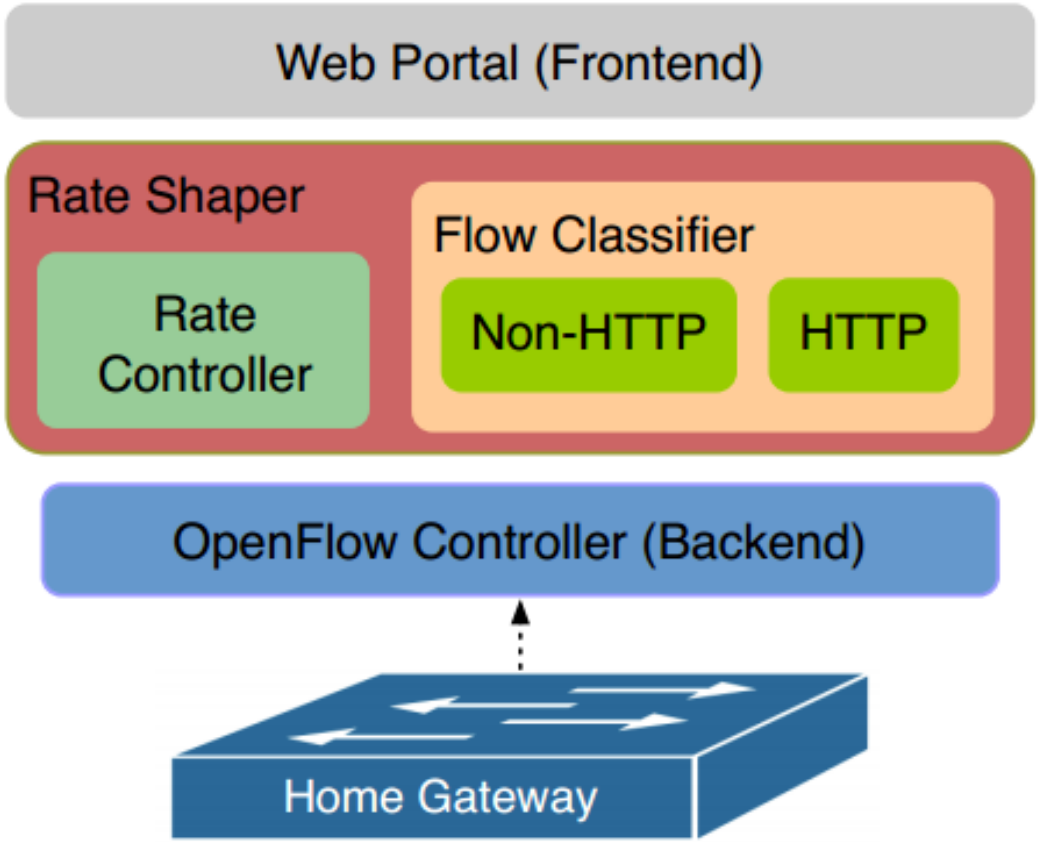


FlowQoS (2014)

FlowQoS : politiques de mise en forme du débit définies par l'utilisateur pour le trafic http

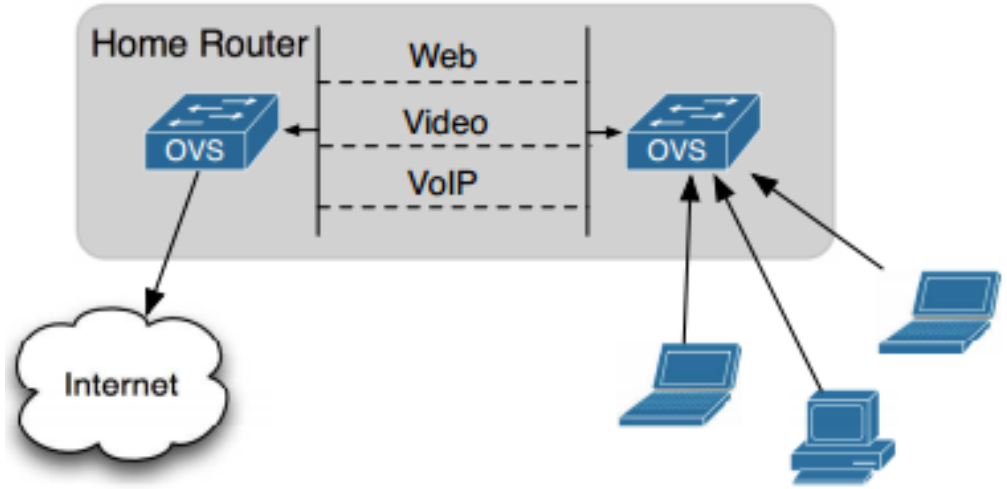
❑ FlowQoS workflow

1. Le contrôleur reçoit packet_in
2. Identifier/classer
   i. port : http ? Classification DNS a et cname
   ii. IP, protocole de transport, classification de la charge utile
3. Affectez le débit au débit approprié défini par le utilisateur
4. Installez les règles appropriées dans les commutateurs



FlowQoS (2014)

- L'attribution d'une priorité à chaque flux en fonction de la configuration de l'utilisateur est compliqué
  - Les routeurs domestiques ne prennent pas en charge le contrôle du débit par débit
  - Des mécanismes tels que tc nécessitent la configuration d'interfaces virtuelles ou le balisage via iptables
  - Open vSwitch ne prend pas encore en charge les parties d'OpenFlow 1.3 spécification qui fournit une QoS par flux
- Une solution de contournement pour ces limitations : – Deux commutateurs virtuels à l'intérieur du routeur domestique.
- Les différentes connexions entre les 2 interrupteurs
  - Configuré via l'utilitaire tc de Linux
  - Différents taux assignés spécifiés par le contrôleur, prédéfinis par l'utilisateur



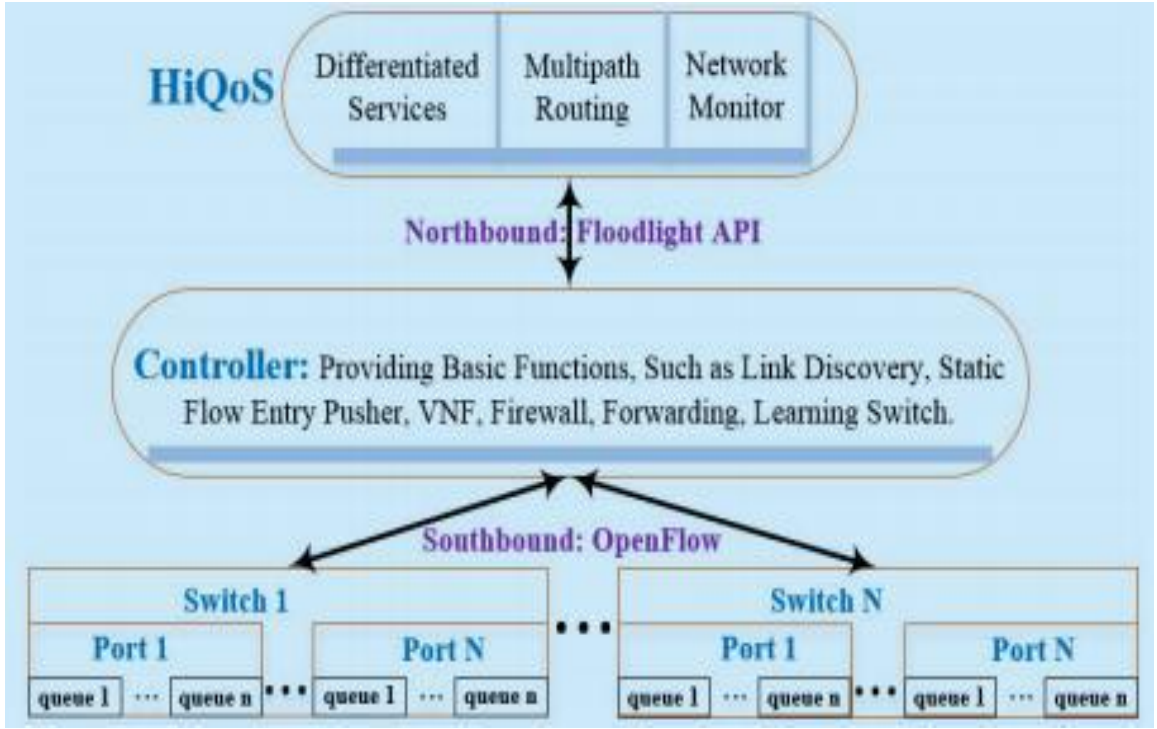
- Lorsqu'un nouveau flux arrive au commutateur, il est redirigé vers le classificateur de flux approprié
- Le classificateur identifie le type d'application pour le flux
- Le contrôleur installe les règles OpenFlow dans l'OVS
- Le commutateur se réfère à ses règles existantes pour déterminer quel intercommutateur la connexion correspond à cette classe de trafic
- Le nouveau flux est acheminé sur les liens virtuels avec les paramètres de mise en forme

HiQoS (2015)

HiQoS : multichemin, mise en file d'attente et reroutage

❑ HiQoS workflow

1. Recevoir packet_in
2. Calculer plusieurs chemins src->dst
   - Dijkstra + CSP
3. Identifier/classer le trafic
   - (ip,port,protocole,…)
4. Choisissez un chemin optimal
   - utilisation minimale de la bande passante d'une file d'attente
5. Mettre en file d'attente



CHAPITRE 2

Etudier les protocoles dans les réseaux SDN

Ce que vous allez apprendre dans ce chapitre :

- Les Protocole dans les réseaux SDN

6 heures

CHAPITRE 2

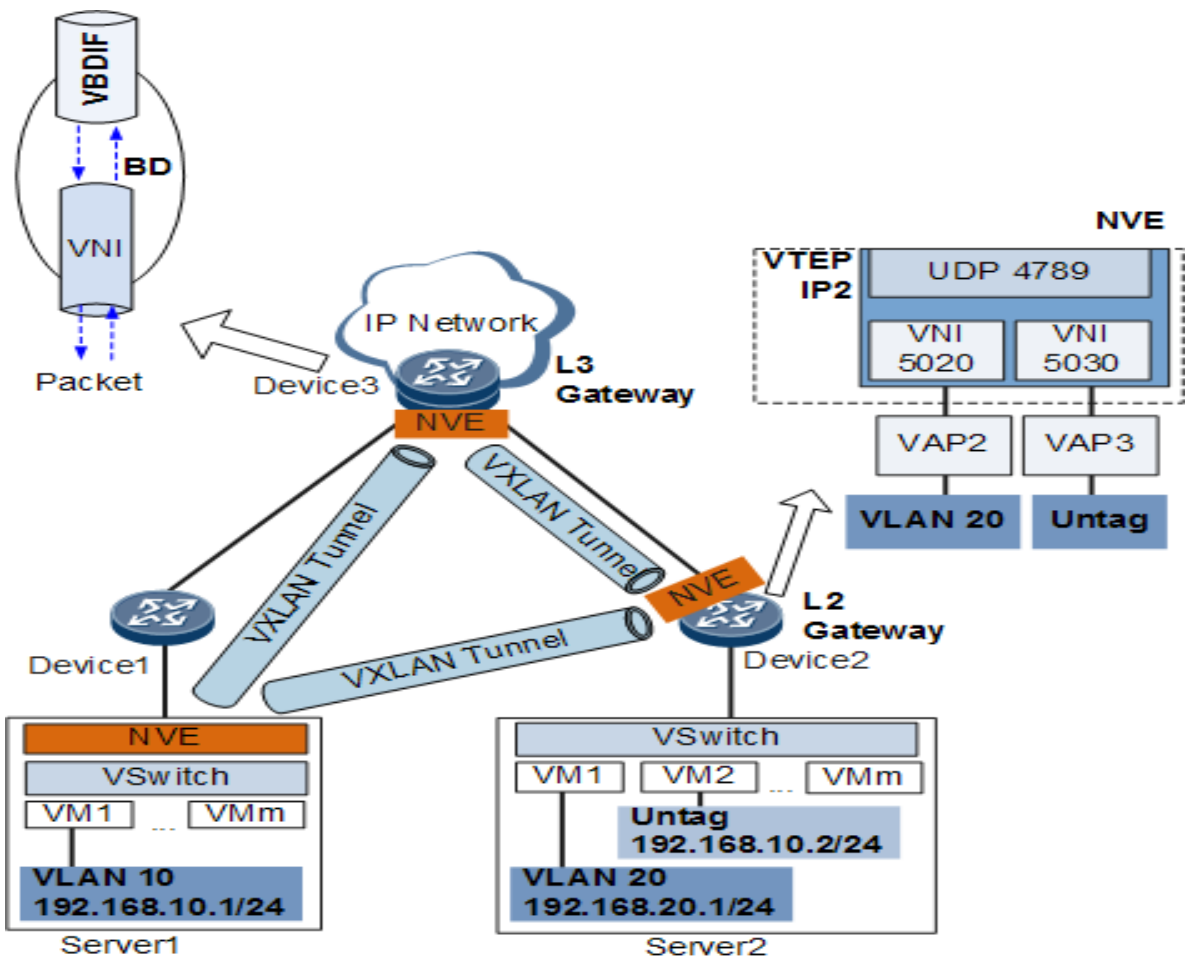
Etudier les protocoles dans les réseaux SDN

1. La technologie VXLAN
2. DMVPN
3. PFR

PARTIE 3

La technologie VXLAN

Le réseau local extensible virtuel (VXLAN) est une technologie de virtualisation de réseau NVO3 qui encapsule les paquets de données envoyés par des machines virtuelles (VM) dans des paquets UDP et encapsule les adresses IP et MAC utilisées sur le réseau physique dans des en-têtes externes avant d'envoyer les paquets sur un réseau IP. Le point de terminaison du tunnel de sortie décapsule ensuite les paquets et envoie les paquets à la machine virtuelle de destination.



Concepts VXLAN

Concept	Description
Réseaux sous-jacents et superposés	VXLAN permet de créer des réseaux virtuels de couche 2 ou de couche 3 (réseaux superposés) sur des réseaux physiques existants (réseaux sous-jacents). Les réseaux superposés utilisent des technologies d'encapsulation pour transmettre les paquets de locataires entre les sites via des chemins de transfert de couche 3 fournis par les réseaux sous-jacents. Les locataires ne connaissent que les réseaux superposés.
Bord de virtualisation réseau (NVE)	Entité réseau déployée à la périphérie du réseau et implémentant les fonctions de virtualisation du réseau. REMARQUE : les vSwitches sur les appareils et les serveurs peuvent fonctionner comme des NVE.
VXLAN tunnel endpoint (VTEP)	Un point de terminaison de tunnel VXLAN qui encapsule et décapsule les paquets VXLAN. Il est représenté par un NVE. Un VTEP se connecte à un réseau physique et se voit attribuer une adresse IP de réseau physique. Cette adresse IP n'est pas pertinente pour les réseaux virtuels. Dans les paquets VXLAN, l'adresse IP source est l'adresse VTEP du nœud local et l'adresse IP de destination est l'adresse VTEP du nœud distant. Cette paire d'adresses VTEP correspond à un tunnel VXLAN.
VXLAN network identifier (VNI)	Un identifiant de segment VXLAN similaire à un ID VLAN. Les machines virtuelles sur différents segments VXLAN ne peuvent pas communiquer directement au niveau de la couche 2. Un VNI identifie un seul locataire. Même si plusieurs utilisateurs de terminaux appartiennent au même VNI, ils sont considérés comme un locataire. Un VNI se compose de 24 bits et prend en charge un maximum de 16 millions de locataires. Un VNI peut être un VNI de couche 2 ou de couche 3. Un VNI de couche 2 est mappé à un BD pour la transmission intra-segment des paquets VXLAN. Un VNI de couche 3 est lié à une instance VPN pour la transmission inter-segment des paquets VXLAN.

Concepts VXLAN

Concept	Description
Bridge domain (BD)	Un domaine de diffusion de couche 2 via lequel les paquets de données VXLAN sont transférés. Les VNI identifiant les VN doivent être mappés aux BD afin qu'un BD puisse fonctionner comme une entité de réseau VXLAN pour transmettre le trafic VXLAN.
VBDIF interface	Une sous-interface de couche 2 utilisée pour transmettre des paquets de données. Les sous-interfaces de couche 2 peuvent avoir différents types d'encapsulation configurés pour transmettre divers types de paquets de données.
Virtual access point (VAP)	Une sous-interface de couche 2 utilisée pour transmettre des paquets de données. Les sous-interfaces de couche 2 peuvent avoir différents types d'encapsulation configurés pour transmettre divers types de paquets de données.
Gateway	Dispositif qui assure la communication entre les VXLAN identifiés par différents VNI et entre les VXLAN et les non-VXLAN. Une passerelle VXLAN peut être une passerelle de couche 2 ou de couche 3. Passerelle de couche 2 : permet aux locataires d'accéder aux VXLAN et à la communication intra-segment sur un VXLAN. Passerelle de couche 3 : permet la communication VXLAN inter-segments et l'accès aux réseaux externes.

CHAPITRE 2

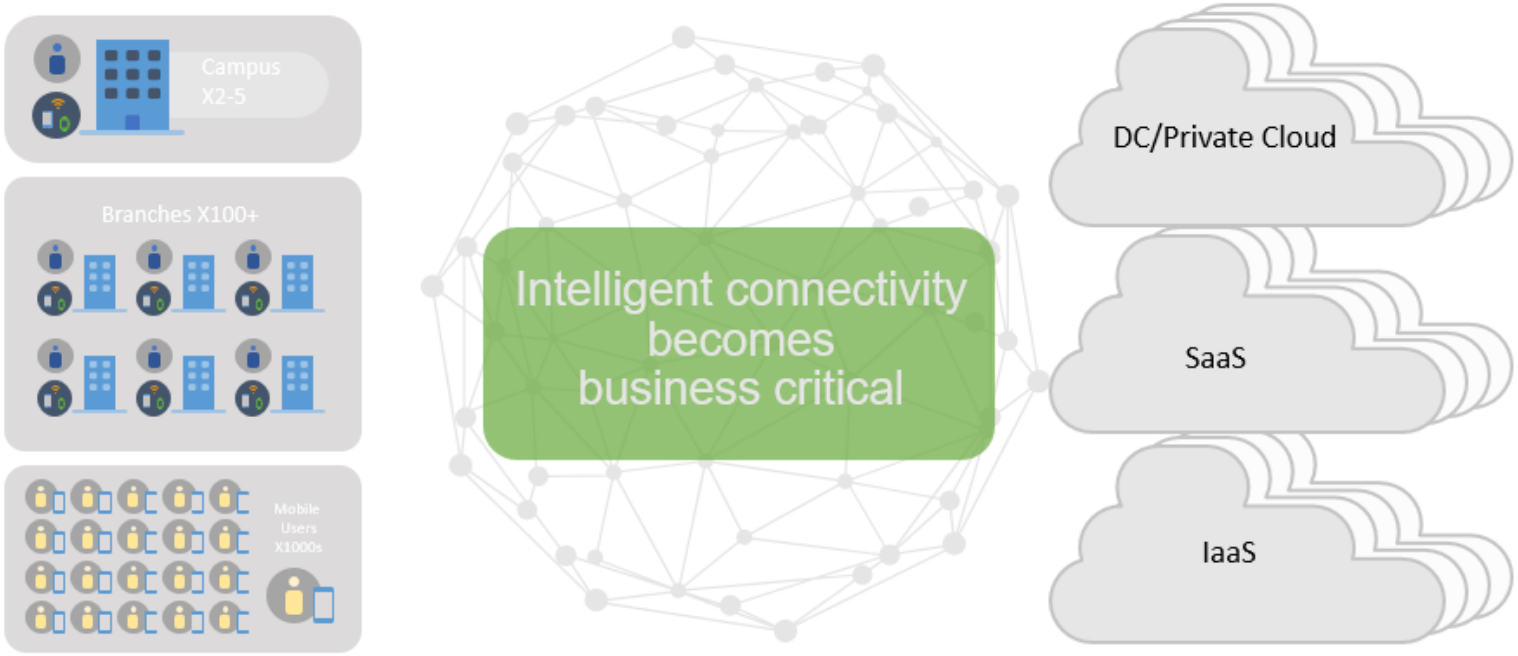
Etudier les protocoles dans les réseaux SDN

1. La technologie VXLAN
2. Les protocoles de l’intelligent WAN

WAN Intelligent

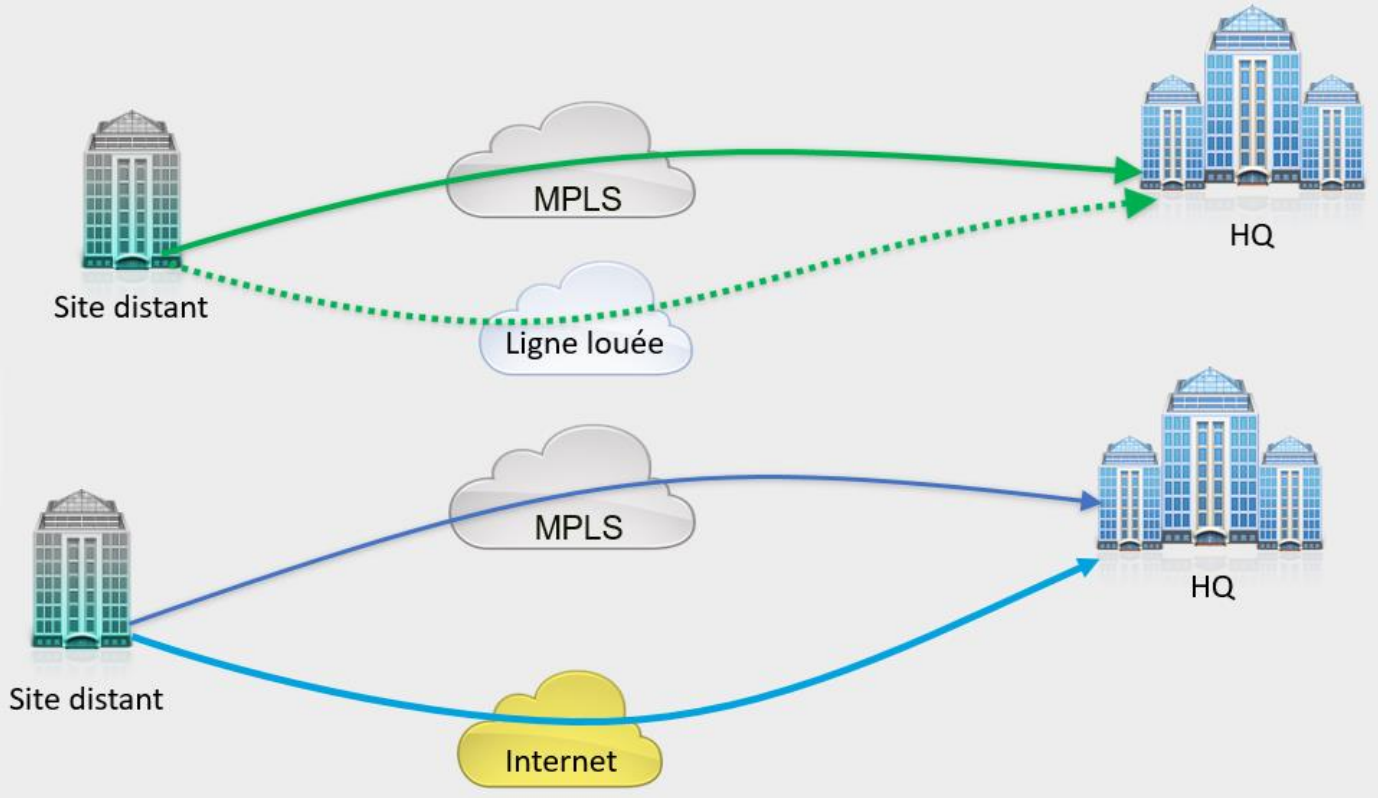
- **Nouvelle architecture WAN**

- Un SDWAN est considérée comme la prochaine génération d'architecture WAN optimisée pour le cloud, l'IOT…
- Contrairement à de nombreuses solutions SD-WAN, IWAN vous permet de déployer rapidement des applications gourmandes en bande passante. Vous pouvez choisir n'importe quel modèle d'opérateur : modèle MPLS, Internet, cellulaire ou hybride.



Modèle d'accès WAN

- Deux fournisseurs de transport WAN pour augmenter la disponibilité du réseau.
- Le service MPLS et le service de ligne loués peuvent être coûteux et ne sont pas toujours rentables en terme de la bande passante,
- Utiliser l'internet comme réseaux de transport sans affecter les performances, la sécurité ou la fiabilité.
    - Aujourd'hui, il est actif / en veille, et on veut passer à actif / actif et obtenir plus de capacité pour notre WAN et pour beaucoup moins d'argent.

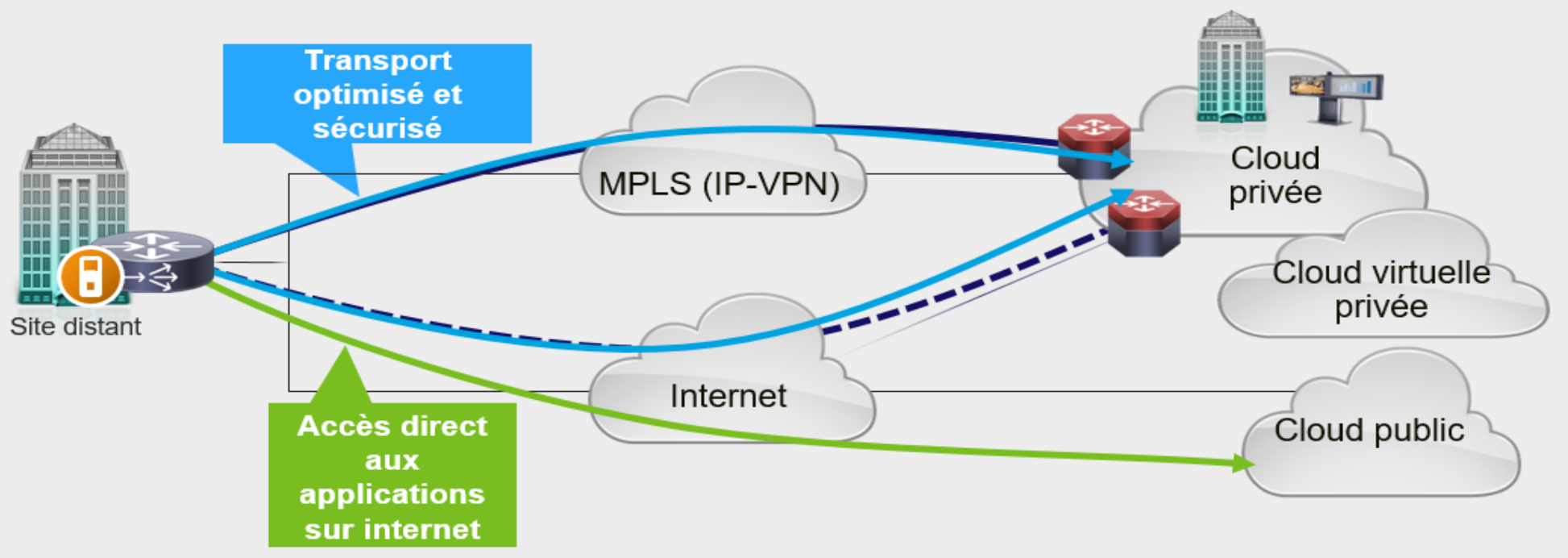


PARTIE 3

MPLS avec SDN

La nouvelle approche du WAN nous permet :

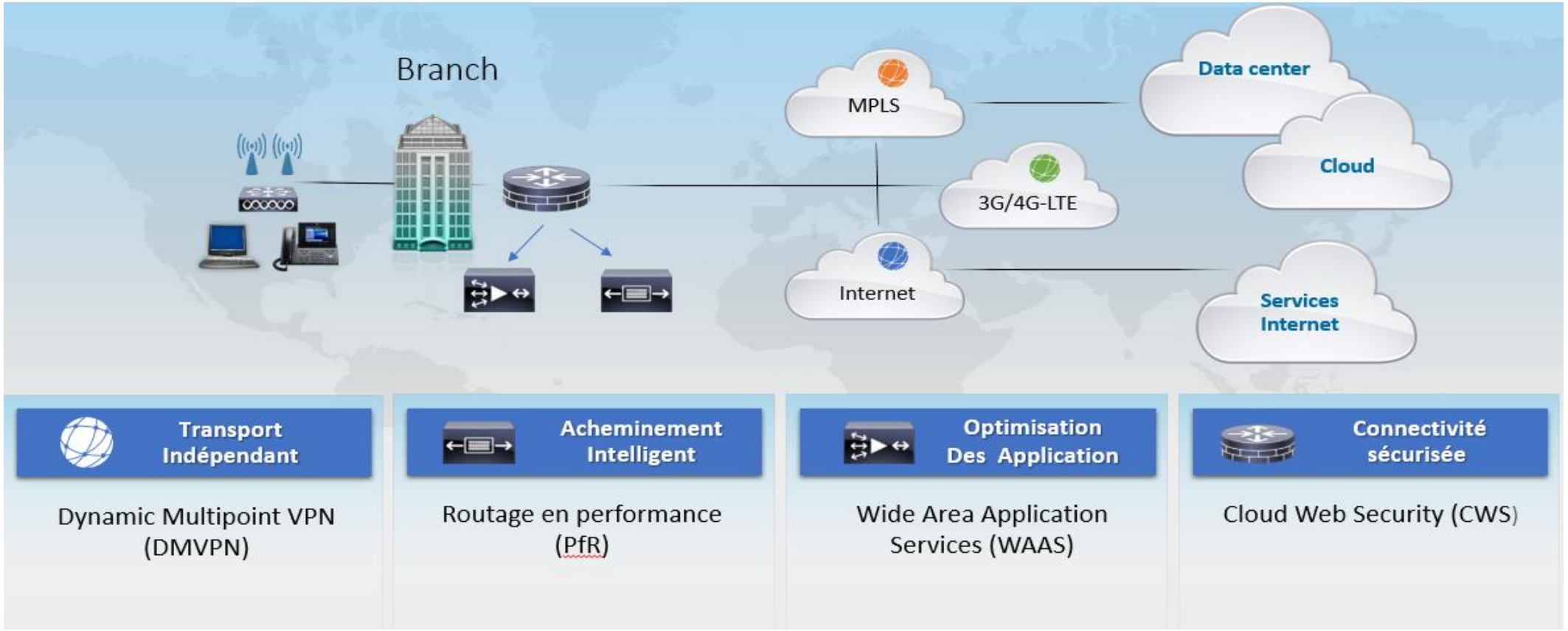
- ✓ Se connecter à un mode plus peu coûteux comme INTERNET pour des données moins importantes.
- ✓ Utiliser l'optimisation d'application, et de sécuriser fortement l'accès Internet direct.



PARTIE 3

La solution IWAN

IWAN Fournit une conception pour les entreprises qui souhaitent déployer un WAN avec transport indépendant, contrôle de chemin intelligent, une optimisation d'application et une connectivité sécurisé.



DMVPN

- C'est un mécanisme qui vous permet d'établir les tunnels IPsec+GRE directement entre les routeurs qui veulent communiquer entre eux avec une simplicité et scalabilité et surtout de façon totalement dynamique!
- Le DMVPN est caractérisé par : design simplifié, connexions dynamiques, sécurité robuste et éprouvée

Les fonctionnalités du DMVPN permet :

- Réduit la complexité du déploiement : offre une configuration zéro-tactile, réduisant considérablement la complexité du déploiement dans les VPN.
- Simplifie les communications entre sites distants : Permet une connectivité directe entre les sites distants pour les applications métier comme la voix.
- Améliore la résilience des entreprises : Empêche la perturbation des applications et des services essentiels aux entreprises en intégrant le routage avec la technologie IPsec.

PARTIE 3

DMVPN

Design simplifié

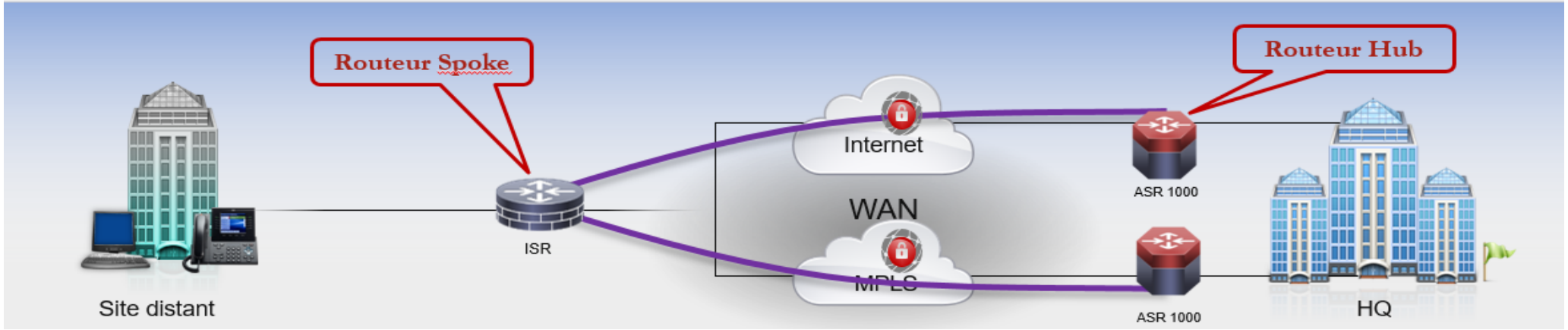
- Offre une configuration zéro-touch

Connexions dynamiques

- Topologies « hub-and-spoke » et de maillage complet évolutives.
- **mGRE**
- **NHRP**

Sécurité robuste éprouvée

- Améliore la résilience des entreprises en intégrant le routage avec l'**IPsec**

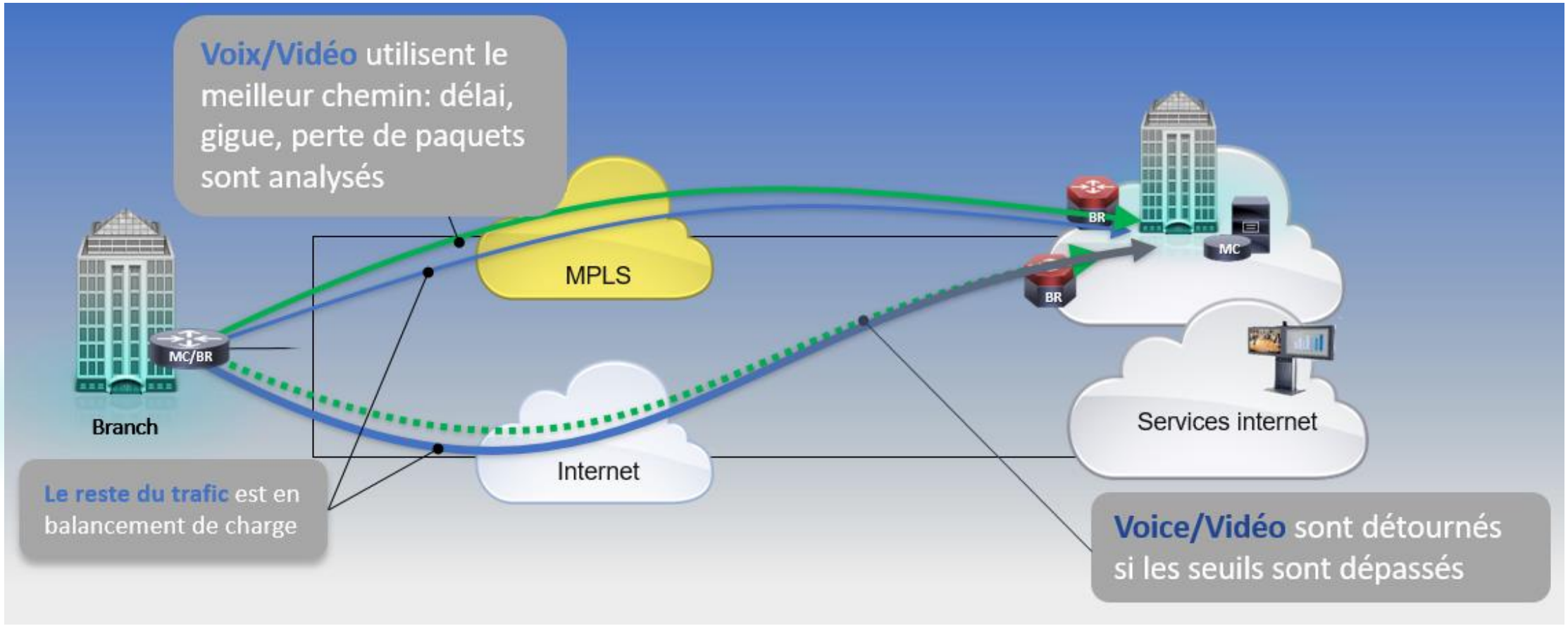


Contrôle intelligent du chemin

- Contrôle dynamiquement les décisions d'acheminement des paquets de données en regardant le type d'application, les performances, les politiques et l'état du chemin d'accès..
- Les routeurs de bordures recueillent des informations sur le trafic et le chemin d'accès et l'envoient au contrôleur principal, qui détecte et applique les règles de service pour correspondre à l'exigence de l'application.

PARTIE 3

Contrôle intelligent du chemin



La technologie WAAS

Contrôle des applications :
- La technologie WAAS (Wide Area Application Services) a pour objectif principal d'améliorer les performances applicatives.

- Problème:

- Latence d'application
- Inefficacité de la bande passante WAN

Réduire la charge: lz, dre, tcp optim.

****

****

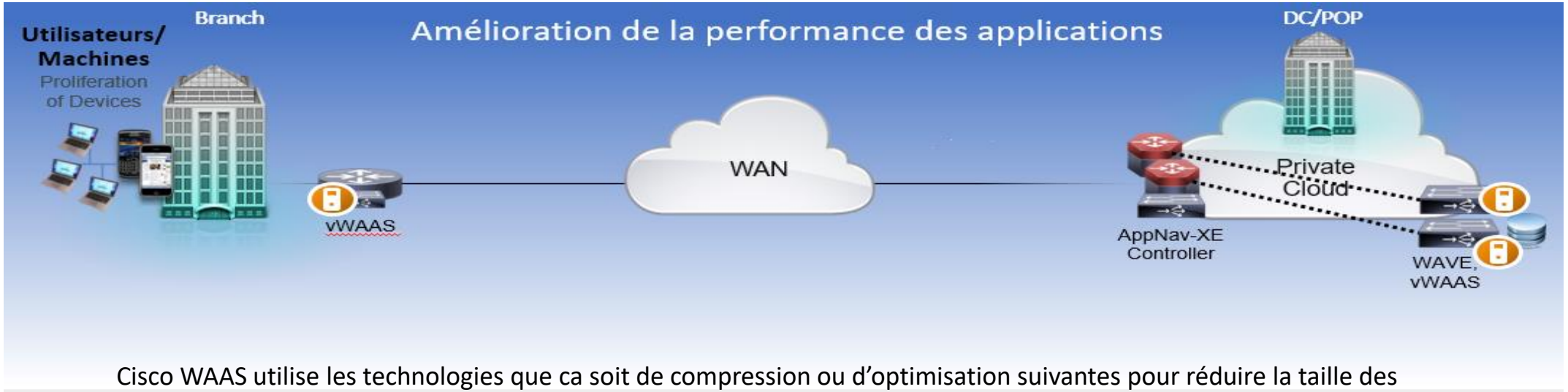
Le système WAAS se compose d'un ensemble d'appareils appelés moteurs (WAE) qui fonctionnent ensemble pour optimiser le trafic TCP sur votre réseau. Lorsque les applications client et serveur tentent de communiquer les unes avec les autres, le réseau intercepte et redirige ce trafic vers les WAE Afin qu'ils puissent agir pour le compte de l'application client et du serveur de destination. Les WAE examinent le trafic et utilisent des règles d'application intégrées pour déterminer s'il faut optimiser le trafic ou lui permettre de passer à travers votre réseau non optimisé.

Cisco WAAS utilise les technologies que ca soit de compression ou d'optimisation suivantes pour réduire la taille des données transmises sur votre WAN:
Élimination des redondances de données (DRE)
Compression LZ

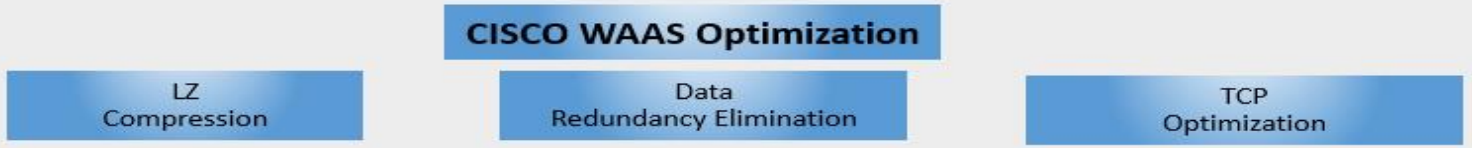
Optimisation TCP

La technologie WAAS

Le système WAAS se compose d'un ensemble d'appareils appelés moteurs (WAE) qui fonctionnent ensemble pour optimiser le trafic TCP sur votre réseau. Lorsque les applications client et serveur tentent de communiquer les unes avec les autres, le réseau intercepte et redirige ce trafic vers les WAE Afin qu'ils puissent agir pour le compte de l'application client et du serveur de destination. Les WAE examinent le trafic et utilisent des règles d'application intégrées pour déterminer s'il faut optimiser le trafic ou lui permettre de passer à travers votre réseau non optimisé.



Cisco WAAS utilise les technologies que ca soit de compression ou d'optimisation suivantes pour réduire la taille des données transmises sur votre WAN:



PARTIE 3

Le service Cisco Cloud Web Security (CWS)

- ✓ Le service Cisco Cloud Web Security (CWS) fournit un proxy Web basé sur le cloud pour gérer de manière centralisée et sécuriser le trafic des utilisateurs qui accèdent à Internet.
- ✓ En tant que service cloud, il offre une très grande flexibilité.
- ✓ Utilisé pour gérer de manière centralisée et sécurisée le trafic des utilisateurs qui accèdent directement à l'internet.
- ✓ Une interface de gestion unique fournit un contrôle global.